Applied Logic for Computer Scientists

Computational Deduction and Formal Proofs

Springer, 2017

doi: http://link.springer.com/book/10.1007%2F978-3-319-51653-0

Answers to Some Exercises

Mauricio Ayala-Rincón and Flávio L. C. de Moura

September 19, 2018

Contents

Introduction

Exercise 1. *Prove these four properties.*

At this point of the discussion we invite you to use your intuition and provide an informal "proof". When more knowledge about formal deduction is provided you migth try this question again.

Exercise 2. (*) *Design an algorithm for computing the function* gcd *in its whole domain:* $\mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}$. *Prove that your algorithm is well-defined and that is correct.*
Hint: assuming the four properties and Euclid's theorem prove that gcd_2 *is algebraically correct in the following sense:*

For all $(i, j) \in \mathbb{Z}^* \times \mathbb{Z}$, *where* $\mathbb{Z}^*$ *denotes the non zero integers,* $\mathrm{gcd}_2(|i|, |j|)$ *computes a number* $k \in \mathbb{N}$, *such that*

- k *divides* i,
- k *divides* j *and*
- *For all* $p \in \mathbb{Z}$ *such that* p *divides both* i *and* j, *it holds that* $p \leq k$.

See the PVS theory `gcd` *in the page of the book. Also for this question you would require elements that are studied in the next chapters.*

Chapter 1

Derivation and Proofs in the Propositional Logic

Exercise 3. *Proof by structural induction that:*

1. *For any prefix s of a well-formed propositional formula ϕ, the number of open parentheses is greater than or equal to the number of closed parentheses in s.*

2. *Any proper prefix s of a well-formed propositional formula ϕ might not be a well-formed propositional formula. By "proper" we understand that s can not be equal to ϕ.*

Exercise 4. *Prove that $\phi \vee \psi \vdash \psi \vee \phi$, i.e., the disjunction is commutative.*

Exercise 5. *Prove that the rule $(\bot_e)$ is not essential, i.e., prove that this rule can be derived from the rules presented in Table 1.3.*

$$\dfrac{\dfrac{\dfrac{\bot \qquad [\neg\varphi]^x}{\bot \wedge \neg\varphi}\,(\wedge_i)}{\bot}\,(\wedge_e)}{\varphi}\,(\text{PBC})\ x$$

Exercise 6. *Build derivations for both versions of contraposition below.*

a. $\neg\psi \to \phi \dashv\vdash \neg\phi \to \psi$ *and*

b. $\psi \to \neg\phi \dashv\vdash \phi \to \neg\psi$.

Exercise 7. *As an exercise, prove that* $((\phi \wedge \psi) \wedge \varphi) \vdash (\phi \wedge (\psi \wedge \varphi))$.

Exercise 8. *As an exercise, prove that* $((\phi \vee \psi) \vee \varphi) \vdash (\phi \vee (\psi \vee \varphi))$.

Exercise 9. *Classify the derived rules of Table 1.4 discriminating those that belong to the intuitionistic fragment of propositional logic, and those that are classical. For instance,* (CP_1) *was proved above using only intuitionistic rules which means that it belongs to the intuitionistic fragment.*
Hint: to prove that a derived rule is not intuitionistic, one can show that using only intuitionistic rules and the derived rule a strictly classical rule such as (PBC) , (LEM) *or* $(\neg\neg_e)$ *can be derived.*

Exercise 10. *Check whether each variant of contraposition below is either an intuitionistic or a classical rule.*

$$\dfrac{\neg\varphi \to \psi}{\neg\psi \to \varphi}\,(\text{CP}_3) \qquad\qquad \dfrac{\varphi \to \neg\psi}{\psi \to \neg\varphi}\,(\text{CP}_4)$$

Exercise 11. *Similarly, check whether each variant of* (MT) below is either an intuitionistic or a classical rule.

$$\dfrac{\varphi \to \neg\psi \qquad \psi}{\neg\varphi}\,(\mathrm{MT}_2) \qquad\qquad \dfrac{\neg\varphi \to \psi \qquad \neg\psi}{\varphi}\,(\mathrm{MT}_3) \qquad\qquad \dfrac{\neg\varphi \to \psi \qquad \neg\psi}{\varphi}\,(\mathrm{MT}_4)$$

Exercise 12. *Using only the rules for the minimal propositional calculus, i.e. the rules in Table 1.2 without* $(\bot_e)$*, give derivations for the following sequents.*

a. $\neg\neg\neg\phi \dashv\vdash \neg\phi$.

$$(\neg_i)\,v\ \dfrac{(\neg_e)\ \dfrac{\neg\neg\neg\phi \qquad (\neg_i)\,u\ \dfrac{(\neg_e)\ \dfrac{[\neg\phi]^u \qquad [\phi]^v}{\bot}}{\neg\neg\phi}}{\bot}}{\neg\phi} \qquad\qquad \dfrac{\dfrac{\neg\phi \qquad [\neg\neg\phi]^u}{\bot}\,(\neg_e)}{\neg\neg\neg\phi}\,(\neg_i)\,u$$

b. $\neg\neg(\phi \to \psi) \vdash (\neg\neg\phi) \to (\neg\neg\psi)$.

A derivation is given below.

$$
\dfrac{\dfrac{\dfrac{\neg\neg(\phi\to\psi) \qquad \dfrac{\dfrac{[\neg\neg\phi]^u \qquad \dfrac{\dfrac{[\neg\psi]^v \qquad \dfrac{[\phi\to\psi]^x \qquad [\phi]^y}{\psi}\,(\to_e)}{\bot}\,(\neg_e)}{\neg\phi}\,(\neg_i)\ y}{\bot}\,(\neg_e)}{\neg(\phi\to\psi)}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\psi}\,(\neg_i)\ v}{(\neg\neg\phi)\to(\neg\neg\psi)}\,(\to_i)\ u
$$

c. $\neg\neg(\phi\wedge\psi) \dashv\vdash (\neg\neg\phi)\wedge(\neg\neg\psi)$.

$$
\begin{prooftree}
\AxiomC{$\neg\neg(\phi \wedge \psi)$}
\AxiomC{$[\neg\phi]^u$}
\AxiomC{$[\phi \wedge \psi]^v$}
\RightLabel{$(\wedge_e)$}
\UnaryInfC{ϕ}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ v$}
\UnaryInfC{$\neg(\phi \wedge \psi)$}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ u$}
\UnaryInfC{$\neg\neg\phi$}
\AxiomC{$\neg\neg(\phi \wedge \psi)$}
\AxiomC{$[\neg\psi]^x$}
\AxiomC{$[\phi \wedge \psi]^y$}
\RightLabel{$(\wedge_e)$}
\UnaryInfC{ψ}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ y$}
\UnaryInfC{$\neg(\phi \wedge \psi)$}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ x$}
\UnaryInfC{$\neg\neg\psi$}
\RightLabel{$(\wedge_i)$}
\BinaryInfC{$(\neg\neg\phi) \wedge (\neg\neg\psi)$}
\end{prooftree}
$$

$$
\begin{prooftree}
\AxiomC{$(\neg\neg\phi) \wedge (\neg\neg\psi)$}
\LeftLabel{$(\wedge_e)$}
\UnaryInfC{$\neg\neg\psi$}
\AxiomC{$(\neg\neg\phi) \wedge (\neg\neg\psi)$}
\LeftLabel{$(\wedge_e)$}
\UnaryInfC{$\neg\neg\phi$}
\AxiomC{$[\phi]^x$}
\AxiomC{$[\psi]^y$}
\LeftLabel{$(\wedge_i)$}
\BinaryInfC{$\phi \wedge \psi$}
\AxiomC{$[\neg(\phi \wedge \psi)]^z$}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ x$}
\UnaryInfC{$\neg\phi$}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ y$}
\UnaryInfC{$\neg\psi$}
\RightLabel{$(\neg_e)$}
\BinaryInfC{$\bot$}
\RightLabel{$(\neg_i)\ z$}
\UnaryInfC{$\neg\neg(\phi \wedge \psi)$}
\end{prooftree}
$$

d. $\neg(\phi \vee \psi) \dashv\vdash (\neg\phi \wedge \neg\psi)$.

From left to right, one has the derivation below.

$$\dfrac{(\neg_i)\,u\;\dfrac{(\neg_e)\;\dfrac{\neg(\phi\lor\psi)\qquad (\lor_i)\,\dfrac{[\phi]^u}{\phi\lor\psi}}{\bot}}{\neg\phi}\qquad\qquad \dfrac{\dfrac{\neg(\phi\lor\psi)\qquad \dfrac{[\psi]^v}{\phi\lor\psi}\,(\lor_i)}{\bot}\;(\neg_e)}{\neg\psi}\;(\neg_i)\,v}{\neg\phi\land\neg\psi}\;(\land_i)$$

From right to left, one has the derivation below.

$$\dfrac{\dfrac{[(\phi\lor\psi)]^u\qquad (\neg_e)\;\dfrac{(\land_e)\;\dfrac{(\neg\phi\land\neg\psi)}{\neg\phi}\qquad [\phi]^x}{\bot}\qquad\qquad \dfrac{\dfrac{(\neg\phi\land\neg\psi)}{\neg\psi}\;(\land_e)\qquad [\psi]^y}{\bot}\;(\neg_e)}{\bot}\;(\lor_e)\,x,y}{\neg(\phi\lor\psi)}\;(\neg_i)\,u$$

e. $\phi\lor\psi\vdash\neg(\neg\phi\land\neg\psi)$.

$$\dfrac{\dfrac{\phi \lor \psi \qquad \dfrac{\dfrac{[\neg\phi \land \neg\psi]^u}{\neg\phi}(\land_e) \qquad [\phi]^x}{\bot}(\neg_e) \qquad \dfrac{\dfrac{[\neg\phi \land \neg\psi]^u}{\neg\psi}(\land_e) \qquad [\psi]^y}{\bot}(\neg_e)}{\bot}(\lor_e)\ x, y}{\neg(\neg\phi \land \neg\psi)}(\neg_i)\ u$$

f. $\vdash \neg\neg(\phi \lor \neg\phi)$.

$$\dfrac{\dfrac{[\neg(\phi \lor \neg\phi)]^u \qquad \dfrac{\dfrac{\dfrac{[\neg(\phi \lor \neg\phi)]^u \qquad \dfrac{[\phi]^v}{(\phi \lor \neg\phi)}(\lor_i)}{\bot}(\neg_e)}{\neg\phi}(\neg_i)\ v}{\phi \lor \neg\phi}(\lor_i)}{\bot}(\neg_e)}{\neg\neg(\phi \lor \neg\phi)}(\neg_i)\ u$$

Exercise 13. *Using the rules for the intuitionistic propositional calculus, that is the rules in Table 1.2, give derivations for the following sequents.*

a. $(\neg\neg\phi) \to (\neg\neg\psi) \vdash \neg\neg(\phi \to \psi)$. *Compare with item b of Exercise 12.*

$$\dfrac{\dfrac{\dfrac{[\neg(\phi\to\psi)]^x \qquad \dfrac{[\psi]^w}{\phi\to\psi}\,(\to_i)\,\emptyset}{\bot}\,(\neg_e)}{\neg\psi}\,(\neg_i)\,w \qquad \dfrac{\neg\neg\phi\to\neg\neg\psi \qquad \dfrac{\dfrac{[\neg(\phi\to\psi)]^x \qquad \dfrac{\dfrac{\dfrac{[\phi]^y \quad [\neg\phi]^z}{\bot}\,(\neg_e)}{\psi}\,(\bot_e)}{\phi\to\psi}\,(\to_i)\,y}{\bot}\,(\neg_e)}{\neg\neg\phi}\,(\neg_i)\,z}{\neg\neg\psi}\,(\to_e)}{\dfrac{\bot}{\neg\neg(\phi\to\psi)}\,(\neg_i)\,x}\,(\neg_e)$$

b. $\vdash \neg\neg(\neg\neg\phi \to \phi)$.

A simple solution is possible from the previous item using a minimal derivation for $\neg\neg\neg\varphi \vdash \neg\varphi$ (Exercise 12 a). Below another intuitionistic derivation.

$$
\dfrac{[\neg(\neg\neg\phi \to \phi)]^u \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg(\neg\neg\phi \to \phi)]^u \qquad \dfrac{[\phi]^x}{\neg\neg\phi \to \phi}\,(\to_i)\ \emptyset}{\bot}\,(\neg_e)}{\neg\phi}\,(\neg_i)\ x \qquad [\neg\neg\phi]^y}{\bot}\,(\neg_e)}{\phi}\,(\bot_e)}{\neg\neg\phi \to \phi}\,(\to_i)\ y}{\dfrac{\bot}{\neg\neg(\neg\neg\phi \to \phi)}\,(\neg_i)\ u}\,(\neg_e)
$$

Exercise 14. (*) *A propositional formula ϕ belongs to the negative fragment if it does not contain disjunctions and all propositional variables occurring in ϕ are preceded by negation. Formulas in this fragment have the following syntax.*

$$\phi ::= (\neg v) \;\;||\;\; \bot \;\;||\;\; (\neg\phi) \;\;||\;\; (\phi \wedge \phi) \;\;||\;\; (\phi \to \phi), \quad \textit{for } v \in V$$

Prove by induction on ϕ, that for any formula in the negative fragment there are derivations in the minimal propositional calculus for

$$\vdash \phi \leftrightarrow \neg\neg\phi$$

i.e. prove $\vdash \phi \to \neg\neg\phi$ and $\vdash \neg\neg\phi \to \phi$.

Let $\vdash_M$ denote derivations in the minimal propositional calculus. The case $\vdash_M \phi \to \neg\neg\phi$ is easy. For the case $\vdash_M \neg\neg\phi \to \phi$, *one uses induction on ϕ and Exercise 12.* **(IB)**

- $\vdash_M \neg\neg\neg v \to \neg v$:

$$\dfrac{\dfrac{\dfrac{[\neg\neg\neg v]^y \qquad \dfrac{[v]^x}{\neg\neg v}\,(\neg\neg_i)}{\bot}\,(\neg_e)}{\neg v}\,(\neg_i)\ x}{\neg\neg\neg v \to \neg v}\,(\to_i)\ y$$

- $\vdash_M \neg\neg\bot \to \bot$:

$$\dfrac{\dfrac{[\neg\neg\bot]^y \qquad \dfrac{[\bot]^x}{\neg\bot}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\bot \to \bot}\,(\to_i)\ y$$

(IS)

- **Case** $(\neg\psi)$. $\vdash_M \neg\neg\neg\psi \to \neg\psi$:

$$\dfrac{\dfrac{\dfrac{[\neg\neg\neg\psi]^y \qquad \dfrac{[\psi]^x}{\neg\neg\psi}\,(\neg\neg_i)}{\bot}\,(\neg_e)}{\neg\psi}\,(\neg_i)\ x}{\neg\neg\neg\psi \to \neg\psi}\,(\to_i)\ y$$

- **Case** $(\psi \wedge \varphi)$. $\vdash_M \neg\neg(\psi \wedge \varphi) \to (\psi \wedge \varphi)$:

First, let ∇_0 the following derivation for $\neg\neg(\psi \wedge \varphi) \vdash_M \neg\neg\psi \wedge \neg\neg\varphi$.

$$\dfrac{\dfrac{\dfrac{[\neg\neg(\psi\wedge\varphi)]^z \qquad \dfrac{\dfrac{[\neg\psi]^u \qquad \dfrac{[\psi\wedge\varphi]^v}{\psi}\,(\wedge_e)}{\bot}\,(\neg_e)}{\neg(\psi\wedge\varphi)}\,(\neg_i)\ v}{\bot}\,(\neg_e)}{\neg\neg\psi}\,(\neg_i)\ u \qquad \dfrac{\dfrac{[\neg\neg(\psi\wedge\varphi)]^z \qquad \dfrac{\dfrac{[\neg\varphi]^x \qquad \dfrac{[\psi\wedge\varphi]^y}{\varphi}\,(\wedge_e)}{\bot}\,(\neg_e)}{\neg(\psi\wedge\varphi)}\,(\neg_i)\ y}{\bot}\,(\neg_e)}{\neg\neg\varphi}\,(\neg_i)\ x}{\neg\neg\psi \wedge \neg\neg\varphi}\,(\wedge_i)$$

By IH, there are derivations ∇_1 for $\neg\neg\psi \vdash_M \psi$ and ∇_2 for $\neg\neg\varphi \vdash_M \varphi$. The proof is obtained as follows:

$$
\dfrac{\dfrac{\begin{array}{c}[\neg\neg(\psi\wedge\varphi)]^z\\ \nabla_0\\ \dfrac{\neg\neg\psi\wedge\neg\neg\varphi}{\neg\neg\psi}\,(\wedge_e)\\ \nabla_{1\,(i.h.)}\\ \psi\end{array}\qquad\begin{array}{c}[\neg\neg(\psi\wedge\varphi)]^z\\ \nabla_0\\ \dfrac{\neg\neg\psi\wedge\neg\neg\varphi}{\neg\neg\varphi}\,(\wedge_e)\\ \nabla_{2\,(i.h.)}\\ \varphi\end{array}}{\psi\wedge\varphi}\,(\wedge_i)}{\neg\neg(\psi\wedge\varphi)\to(\psi\wedge\varphi)}\,(\to_i)\;z
$$

- **Case** $(\psi\to\varphi)$. $\vdash_M \neg\neg(\psi\to\varphi)\to(\psi\to\varphi)$: *First, let* ∇_0 *be the derivation below for* $\neg\neg(\psi\to\varphi)\vdash_M(\neg\neg\psi\to\neg\neg\varphi)$.

$$
\dfrac{\dfrac{\dfrac{[\neg\neg(\psi\to\varphi)]^z\qquad\dfrac{\dfrac{[\neg\neg\psi]^u\qquad\dfrac{\dfrac{[\neg\varphi]^v\qquad\dfrac{[\psi\to\varphi]^x\qquad[\psi]^y}{\varphi}\,(\to_e)}{\bot}\,(\neg_e)}{\neg\psi}\,(\neg_i)\;y}{\bot}\,(\neg_e)}{\neg(\psi\to\varphi)}\,(\neg_i)\;x}{\bot}\,(\neg_e)}{\neg\neg\varphi}\,(\neg_i)\;v}{\neg\neg\psi\to\neg\neg\varphi}\,(\to_i)\;u
$$

By IH, there exists a derivation ∇_1 for $\neg\neg\varphi \vdash_M \varphi$. The proof is obtained as follows:

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}[\neg\neg(\psi \to \varphi)]^z \\ \nabla_0 \\ \neg\neg\psi \to \neg\neg\varphi\end{array} \qquad \dfrac{[\psi]^x}{\neg\neg\psi}\,(\neg\neg_i)}{\begin{array}{c}\neg\neg\varphi \\ \nabla_{1\,(i.h.)} \\ \varphi\end{array}}\,(\to_e)}{(\psi \to \varphi)}\,(\to_i)\; x}{\neg\neg(\psi \to \varphi) \to (\psi \to \varphi)}\,(\to_i)\; z$$

Exercise 15. *Give deductions for the following sequents:*

a. $\neg(\neg\phi \wedge \neg\psi) \vdash \phi \vee \psi$.

One uses the derivation below in which ∇ denotes the derivation for $\neg(\phi \vee \psi) \vdash (\neg\phi) \wedge (\neg\psi)$ in exercise 12. Notice that rule (PBC) that is a classical rule is used in this derivation.

$$\dfrac{\dfrac{\neg((\neg\phi) \wedge (\neg\psi)) \qquad \begin{array}{c}\neg(\phi \vee \psi) \\ \nabla \\ (\neg\phi) \wedge (\neg\psi)\end{array}}{\bot}\,(\neg_e)}{\phi \vee \psi}\,(\text{PBC})\; u$$

b. Peirce's law: $\vdash ((\phi \to \psi) \to \phi) \to \phi$.

$$\dfrac{\dfrac{\dfrac{[\neg\phi]^u \qquad \dfrac{[((\phi\to\psi)\to\phi)]^x \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg\phi]^u}{\neg\psi\to\neg\phi}(\to_i)\,\emptyset \qquad [\neg\psi]^v}{\neg\phi}(\to_e) \qquad [\phi]^w}{\bot}(\neg_e)}{\psi}(\text{PBC})\,v}{\phi\to\psi}(\to_i)\,w}{\phi}(\to_e)}{\bot}(\neg_e)}{\phi}(\text{PBC})\,u}{((\phi\to\psi)\to\phi)\to\phi}(\to_i)\,x$$

Exercise 16. (*) *Let Γ be a set, and φ be a formula of propositional logic. Prove that if φ has a classical proof from the assumptions in Γ then $\neg\neg\varphi$ has an intuitionistic proof from the same assumptions. This fact is known as Glivenko's theorem (1929).*

Induction on the derivation $\Gamma \vdash_c \varphi$. Consider the last applied rule as follows:

- $(\wedge_i)$: In this case, φ is of the form $\varphi_1 \wedge \varphi_2$ and $\Gamma \vdash_c \varphi$ is as follows:

$$\dfrac{\begin{matrix}\Gamma\\ \nabla\\ \varphi_1\end{matrix} \qquad \begin{matrix}\Gamma\\ \nabla\\ \varphi_2\end{matrix}}{\varphi_1 \wedge \varphi_2}\ (\wedge_i)$$

By i.h. one has $\Gamma \vdash_i \neg\neg\varphi_i$ $(i = 1, 2)$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{matrix}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_2\end{matrix} \qquad \dfrac{\dfrac{\begin{matrix}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_1\end{matrix} \qquad \dfrac{\dfrac{[\neg(\varphi_1 \wedge \varphi_2)]^x \qquad \dfrac{[\varphi_1]^y \qquad [\varphi_2]^z}{\varphi_1 \wedge \varphi_2}\ (\wedge_i)}{\bot}\ (\neg_e)}{\neg\varphi_1}\ (\neg_i)\ y}{\bot}\ (\neg_e)}{\neg\varphi_2}\ (\neg_i)\ z}{\bot}\ (\neg_e)}{\neg\neg(\varphi_1 \wedge \varphi_2)}\ (\neg_i)\ x$$

- $(\wedge_e)$:

$$\dfrac{\begin{array}{c}\Gamma\\ \nabla\\ \varphi \wedge \psi\end{array}}{\varphi}\ (\wedge_e)$$

By i.h. one has $\Gamma \vdash_i \neg\neg(\varphi \wedge \psi)$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg(\varphi \wedge \psi)\end{array}}{(\neg\neg\varphi) \wedge (\neg\neg\psi)}\ \text{EXERCISE 12}}{\neg\neg\varphi}\ (\wedge_e)$$

- $(\vee_i)$: In this case, one has that φ is of the form $\varphi_1 \vee \varphi_2$, and hence:

$$\dfrac{\begin{array}{c}\Gamma\\ \nabla\\ \varphi_1\end{array}}{\varphi_1 \vee \varphi_2}\ (\vee_i)$$

By i.h. one has $\Gamma \vdash_i \neg\neg\varphi_i$ $(i = 1, 2)$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_1\end{array} \qquad \dfrac{\dfrac{[\neg(\varphi_1\vee\varphi_2)]^x \qquad \dfrac{[\varphi_1]^y}{\varphi_1\vee\varphi_2}\,(\vee_i)}{\bot}\,(\neg_e)}{\neg\varphi_1}\,(\neg_i)\ y}{\bot}\,(\neg_e)}{\neg\neg(\varphi_1\vee\varphi_2)}\,(\neg_i)\ x$$

- $(\vee_e)$:

$$\dfrac{\begin{array}{c}\Gamma\\ \nabla\\ (\varphi_1\vee\varphi_2)\end{array} \qquad \begin{array}{c}[\varphi_1]^x,\Gamma\\ \nabla\\ \varphi\end{array} \qquad \begin{array}{c}[\varphi_2]^y,\Gamma\\ \nabla\\ \varphi\end{array}}{\varphi}\,(\vee_e)\ x,y$$

By i.h. one has $\Gamma\vdash_i\neg\neg(\varphi_1\vee\varphi_2)$ e $\Gamma,[\varphi_i]\vdash_i\neg\neg\varphi$ $(i=1,2)$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg(\varphi_1 \vee \varphi_2)\end{array} \qquad \dfrac{\dfrac{[\neg\varphi]^w \qquad \dfrac{\begin{array}{c}\Gamma\ [\varphi_1]^y\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi\end{array} \quad \begin{array}{c}\Gamma\ [\varphi_2]^z\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi\end{array} \quad [\varphi_1 \vee \varphi_2]^x}{\neg\neg\varphi}\,(\vee_e)\ y,z}{\bot}\,(\neg_e)}{\neg(\varphi_1 \vee \varphi_2)}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\varphi}\,(\neg_i)\ w$$

- $(\to_i)$: In this case, φ is of the form $\varphi_1 \to \varphi_2$, and one has the following derivation:

$$\dfrac{\begin{array}{c}\Gamma \quad [\varphi_1]^x\\ \nabla\\ \varphi_2\end{array}}{\varphi_1 \to \varphi_2}\,(\to_i)$$

By i.h. one has $\Gamma, \varphi_1 \vdash_i \neg\neg\varphi_2$, and we conclude as follows:

$$
\dfrac{\dfrac{\dfrac{\dfrac{[\neg\neg\varphi_1]^w \qquad \dfrac{\dfrac{[\neg\varphi_2]^z \qquad \begin{array}{c}\Gamma\ [\varphi_1]^x\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_2\end{array}}{\bot}\,(\neg_e)}{\neg\varphi_1}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\varphi_2}\,(\neg_i)\ z}{(\neg\neg\varphi_1) \to (\neg\neg\varphi_2)}\,(\to_i)\ w}{\neg\neg(\varphi_1 \to \varphi_2)}\ \textsc{Exercise 13}
$$

- $(\to_e)$:

$$
\dfrac{\begin{array}{c}\Gamma\\ \nabla\\ \varphi_1 \to \varphi\end{array} \qquad \begin{array}{c}\Gamma\\ \nabla\\ \varphi_1\end{array}}{\varphi}\ (\to_e)
$$

By i.h. one has $\Gamma \vdash_i \neg\neg\varphi_1$ and $\Gamma \vdash_i \neg\neg(\varphi_1 \to \varphi)$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg(\varphi_1 \to \varphi)\end{array} \qquad \dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_1\end{array} \qquad \dfrac{[\varphi_1 \to \varphi]^x \qquad [\neg\varphi]^y}{\neg\varphi_1}\,(\text{MT})}{\bot}\,(\neg_e)}{\neg(\varphi_1 \to \varphi)}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\varphi}\,(\neg_i)\ y$$

Despite cases for negation could be omitted since $\neg\varphi$ abbreviates $\varphi \to \bot$, they are included below.

- $(\neg_i)$:

  In this case, φ is of the form $\neg\varphi_1$, and one has the following derivation:

$$\dfrac{\begin{array}{c}\Gamma \quad [\varphi_1]^x\\ \hline \searrow\ \swarrow\\ \bot\end{array}}{\neg\varphi_1}\qquad (\neg_i)\ x$$

  By i.h. one has $\Gamma, \varphi_1 \vdash_i \neg\neg\bot$, and we conclude as follows:

$$\dfrac{\dfrac{[\neg\neg\varphi_1]^y \qquad \dfrac{\dfrac{\begin{array}{c}\Gamma\ [\varphi_1]^x\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\bot\end{array} \qquad \dfrac{[\bot]^z}{\neg\bot}\,(\neg_i)\ z}{\bot}\,(\neg_e)}{\neg\varphi_1}\,(\neg_i)\ x}{\bot}\,(\neg_e)}{\neg\neg\neg\varphi_1}\,(\neg_i)\ y$$

- $(\neg_e)$: in this case we start from the following classical derivation:

$$\dfrac{\begin{array}{c}\Gamma\\ \triangledown\\ \neg\varphi_1\end{array} \qquad \begin{array}{c}\Gamma\\ \triangledown\\ \varphi_1\end{array}}{\bot}\,(\neg_e)$$

By i.h. we have $\Gamma \vdash_i \neg\neg\neg\varphi_1$ and $\Gamma \vdash_i \neg\neg\varphi_1$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\neg\varphi_1\end{array} \qquad \begin{array}{c}\Gamma\\ \nabla_{\text{(i.h.)}}\\ \neg\neg\varphi_1\end{array}}{\bot}\,(\neg_e)}{\neg\neg\bot}\,(\neg\neg_i)$$

- (PBC):

$$\dfrac{\begin{array}{c}\Gamma \quad [\neg\varphi]^x \\ \nabla \\ \bot\end{array}}{\varphi}\ (\text{PBC})\ x$$

By i.h. one has $\Gamma, \neg\varphi \vdash_i \neg\neg\bot$, and we conclude as follows:

$$\dfrac{\dfrac{\begin{array}{c}\Gamma\ [\neg\varphi]^y \\ \nabla_{\text{(i.h.)}} \\ \neg\neg\bot\end{array} \qquad \dfrac{[\bot]^x}{\neg\bot}\ (\neg_i)\ x}{\bot}\ (\neg_e)}{\neg\neg\varphi}\ (\neg_i)\ y$$

Exercise 17. (*) *Consider the negative Gödel translation from classical propositional logic to intuitionistic propositional logic given by:*

- $\bot^n = \bot$
- $p^n = \neg\neg p$, *if* p *is a propositional variable.*
- $(\varphi \wedge \psi)^n = \varphi^n \wedge \psi^n$
- $(\varphi \vee \psi)^n = \neg\neg(\varphi^n \vee \psi^n)$

- $(\varphi \to \psi)^n = \varphi^n \to \psi^n$

Prove that if $\Gamma \vdash \varphi$ *in classical propositional logic then* $\Gamma^n \vdash \varphi^n$ *in intuitionistic propositional logic.*

Hint: for the negation, use that $(\neg\varphi)$ is an abreviation for $\varphi \to \bot$, thus $(\varphi \to \bot)^n = \varphi^n \to \bot$, which means that $(\neg\varphi)^n = \neg\varphi^n$.

Exercise 18. *Prove the following sequent, the double negation of Peirce's law, in the intuitionistic propositional logic:* $\vdash \neg\neg(((\phi \to \psi) \to \phi) \to \phi)$

$$\begin{array}{c}
\dfrac{\dfrac{\dfrac{[\neg\phi]^u \qquad \dfrac{\begin{array}{c}[\neg\neg((\phi\to\psi)\to\phi)]^x \\ \vdots\ \text{(Ex. 12 b.)} \\ \neg\neg(\phi\to\psi)\to\neg\neg\phi\end{array} \qquad \begin{array}{c}\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg\phi]^u}{\neg\psi\to\neg\phi}(\to_i)\,\emptyset \qquad [\neg\psi]^v}{\neg\phi}(\to_e) \qquad [\neg\neg\phi]^w}{\bot}(\neg_e)}{\neg\neg\psi}(\neg_i)\,v}{\neg\neg\phi\to\neg\neg\psi}(\to_i)\,w \\ \vdots\ \text{(Ex. 13 a.)} \\ \neg\neg(\phi\to\psi)\end{array}}{\neg\neg\phi}(\to_e)}{\bot}(\neg_e)}{\neg\neg\phi}(\neg_i)\,u}{\neg\neg((\phi\to\psi)\to\phi)\to\neg\neg\phi}(\to_i)\,x \\
\vdots\ \text{(Ex. 13 a.)} \\
\neg\neg(((\phi\to\psi)\to\phi)\to\phi)
\end{array}$$

Exercise 19. *Prove the previous corollary.*

Exercise 20. *Build a derivation for the instance of Peirce's law in propositional variables* p *and* q *according to the inductive construction of the proof of the completeness (Theorem 4). That is, first build derivations for* $p, q \vdash ((p \to q) \to p) \to p$, $p, \neg q \vdash ((p \to q) \to p) \to p$, $\neg p, q \vdash ((p \to q) \to p) \to p$ *and* $\neg p, \neg q \vdash ((p \to q) \to p) \to p$, *and then assemble these proofs to obtain a derivation for* $\vdash ((p \to q) \to p) \to p$.

Additional Exercise 21. *As explained before, the classical propositional logic can be characterized by any of the equivalent rules* (PBC), $(\neg\neg_e)$ or (LEM). Show that Peirce's law is also equivalent to any of these rules. In other words, build intuitionistic proofs for the rules (PBC), $(\neg\neg_e)$ and (LEM) assuming the rule:

$$\frac{}{((\phi \to \psi) \to \phi) \to \phi}\ \text{(LP)}$$

Next, prove (LP) in three different ways: each proof should be done in the intuitionistic logic assuming just one of (PBC), $(\neg\neg_e)$ and (LEM) at a time.

Additional Exercise 22. *Prove the following sequents:*

a. $\phi \to (\psi \to \gamma), \phi \to \psi \vdash \phi \to \gamma$

b. $(\phi \vee (\psi \to \phi)) \wedge \psi \vdash \phi$

c. $\phi \to \psi \vdash ((\phi \wedge \psi) \to \phi) \wedge (\phi \to (\phi \wedge \psi))$

d. $\vdash \psi \to (\phi \to (\phi \to (\psi \to \phi)))$

Chapter 2

Derivations and Proofs in the Predicate Logic

Exercise 23.

a. *Consider a predicate formula* φ *and a term* t. *Prove that there are no bound variables in the new occurrences of* t *in the formula* $\varphi[x/t]$. *For doing this use induction on the structure of* φ. *Of course, occurrences of the term* t *in the original formula* φ *might be under the scope of quantifiers and consequently variables occurring in these subterms would be bound.*

b. *Let* k *be the number of free occurrences of the variable* x *in the predicate formula* φ. *Prove, also by induction on* φ, *that the size of the term* $\varphi[x/t]$ *is given by* $k|t| + |\varphi| - k$.

c. *For* $x \neq y$, *prove also that:*

   i. $\varphi[x/s][x/t] = \varphi[x/s[x/t]]$;

   ii. $\varphi[x/s][y/t] = \varphi[x/s[y/t]][y/t]$, *if* $y \notin \mathtt{var}(t)$;

   iii. $\varphi[x/s][y/t] = \varphi[y/t][x/s]$, *if* $x \notin \mathtt{var}(t)$ *and* $y \notin \mathtt{var}(s)$.

Exercise 24. *Prove intuitionistically that* $\neg\exists_x\varphi \dashv\vdash \forall_x\neg\varphi$.

$\forall_x\neg\varphi \vdash \neg\exists_x\varphi$:

$$\dfrac{\dfrac{[\exists_x\varphi]^u \qquad \dfrac{[\varphi[x/y]]^w \qquad \dfrac{\forall_x\neg\varphi}{\neg\varphi[x/y]}\,(\forall_e)}{\bot}\,(\neg_e)}{\bot}\,(\exists_e)\ w}{\neg\exists_x\varphi}\,(\neg_i)\ u$$

$\neg\exists_x\varphi \vdash \forall_x\neg\varphi$:

$$\dfrac{\dfrac{\dfrac{\neg\exists_x\varphi \qquad \dfrac{[\varphi[x/y]]^u}{\exists_x\varphi}\,(\exists_i)}{\bot}\,(\neg_e)}{\neg\varphi[x/y]}\,(\neg_i)\ u}{\forall_x\neg\varphi}\,(\forall_i)$$

Exercise 25. *Prove that:*

a. *if x does not occur free in ψ then prove that $(\exists_x\phi) \to \psi \vdash \forall_x(\phi \to \psi)$; and* TBD *b. if x does not occur free in ψ then prove that $(\forall_x \phi) \to \psi \vdash \exists_x(\phi \to \psi)$.*

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\phi[x/x_0]]^u \qquad [\neg\phi[x/x_0]]^v}{\bot}\,(\neg_e)}{\psi}\,(\bot_e)}{\phi[x/x_0] \to \psi}\,(\to_i)\ u}{\exists_x(\phi \to \psi)}\,(\exists_i) \qquad [\neg\exists_x(\phi \to \psi)]^w}{\bot}\,(\neg_e)}{\phi[x/x_0]}\,(\text{PBC})\ v}{\forall_x \phi}\,(\forall_i) \qquad (\forall_x \phi) \to \psi}{\psi}\,(\to_e)}{\phi[x/x_0] \to \psi}\,(\to_i)\ \emptyset}{\exists_x(\phi \to \psi)}\,(\exists_i) \qquad [\neg\exists_x(\phi \to \psi)]^w}{\bot}\,(\neg_e)}{\exists_x(\phi \to \psi)}\,(\text{PBC})\ w
$$

Exercise 26. *Prove that:*

a. $(\forall_x \phi) \land (\forall_x \psi) \dashv\vdash \forall_x(\phi \land \psi)$*; and*

b. $(\exists_x \phi) \lor (\exists_x \psi) \dashv\vdash \exists_x(\phi \lor \psi)$.

Exercise 27. *Prove that* $\forall_x(p(x) \to \neg q(x)) \vdash \neg(\exists_x(p(x) \land q(x)))$.

Exercise 28. *Prove that there exist derivations for* $\neg\neg\varphi \vdash \varphi$ *using only the minimal natural deduction rules and each of the assumptions:*

a. $\neg\exists_x\neg\varphi \to \forall_x\varphi$ *and*

b. $\neg\forall_x\neg\varphi \to \exists_x\varphi$.

Hint: you can choose the variable x *as any variable that does not occurs in* φ*. Thus, the application of rule* $(\exists_e)$ *over the existential formula* $\exists_x\varphi$ *has as witness assumption* $[\varphi[x/x_0]]^w$ *that has no occurrences of* x_0.

a. We use minimal rules and assume the existence of a derivation for $\neg\exists_x\neg\varphi \vdash \forall_x\varphi$*:*

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\exists_x\neg\varphi]^u \qquad [\neg\varphi[x/y]]^w}{\neg\varphi}\,(\exists_e)\ w \qquad \neg\neg\varphi}{\bot}\,(\neg_e)}{\neg\exists_x\neg\varphi}\,(\neg_i)\ u}{\forall_x\varphi}\,\text{ASSUMPTION}}{\varphi}\,(\forall_e)$$

Notice that the application of rule $(\exists_e)$ *above is justified because a variable* x *might be selected that does not occur in* φ*; hence, also the witness variable* y *does not occur in* $\neg\varphi[x/y]$.

b. As in the previous item, we use minimal rules and assume the existence of a derivation for $\neg\forall_x\neg\varphi \vdash \exists_x\varphi$*:*

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\forall_x\neg\varphi]^u}{\neg\varphi}\,(\forall_e)\qquad \neg\neg\varphi}{\bot}\,(\neg_e)}{\neg\forall_x\neg\varphi}\,(\neg_i)\; u}{\exists_x\varphi}\,\text{ASSUMPTION}\qquad\qquad [\varphi[x/y]]^w}{\varphi}\,(\exists_e)\; w$$

The justification for the application of rule $(\exists_e)$ *above is the same as for the previous item.*

Exercise 29. *To complete* $\neg\forall_x\varphi \dashv\vdash \exists_x\neg\varphi$ *(see Example 12), prove that* $\neg\forall_x\varphi \vdash \exists_x\neg\varphi$*.*

Exercise 30. *Complete all other cases of the proof of the Theorem 6 of soundness of predicate logic.*

Exercise 31. *Complete the analysis well-definedness for all the items in the interpretation of formulas* I_Γ*, for a set* Γ *that contains witnesses and is maximally complete.*

Exercise 32. (*) *Research in the suggested related references how a consistent set built over a countable set of symbols, but that uses infinite free variables can be extended to a maximal consistent set with witnesses. The problem, is that in this case there are no new variables that can be used as witnesses. Thus, one needs to extend the language with new constant symbols that will act as witnesses, but each time a new constant symbol is added to the language the set of existential formulas change.*

We invite the reader to review the related references given in the Chapter on suggested reading.

Exercise 33. (*) *Research the general case in which the language is not restricted, that is the case in which* Γ *is built over a non countable set of symbols.*

We invite the reader to review the related references given in the Chapter on suggested reading.

Exercise 34. *Prove that there is no predicate formula φ that holds exclusively for all finite interpretations.*

Exercise 35. *Let E be a binary predicate symbol, e a constant and $\cdot$ and -1 be binary and unary function symbols, respectively. The theory of groups is given by the models of the set of formulas Γ_G:*

$$\forall_x \; E(x,x)$$
$$\forall_{x,y} \; (E(x,y) \rightarrow E(y,x))$$
$$\forall_{x,y,z} \; (E(x,y) \wedge E(y,z) \rightarrow E(x,z))$$
$$\forall_x \; E(x \cdot e, x)$$
$$\forall_x \; E(x \cdot x^{-1}, e)$$
$$\forall_{x,y,z} \; E((x \cdot y) \cdot z, x \cdot (y \cdot z))$$

Notice that according to the three first axioms the symbol E should be interpreted as an equivalence relation such as the equality. Indeed, the three other axioms are those related with group theory itself: the fourth one states the existence of an identity element, the fifth one the inverse function and the sixth one the associativity of the binary operation.

Prove the existence of infinite models by proving that for any $n \in \mathbb{N}$, the structure of arithmetic modulo n is a group of cardinality n. The elements of this structure are all integers modulo n (i.e. the set $\{0, 1, \ldots, n\text{-}1\}$), with addition and identity element 0.

Exercise 36. *A graph is a structure of the form $G = \langle V, E \rangle$, where V is a finite set of vertices and $E \subset V \times V$ a set of edges between the vertices. The problem of reachability in graphs is the question whether there exists a finite path of consecutive edges, say $(u, u_1), (u_1, u_2), \ldots, (u_{n-1}, v)$, between two given nodes $u, v \in V$.*

Prove that there is no predicate formula that expresses reachability in graphs.
Hint: the key observation to conclude is that the problem of reachability between two nodes might be answered positively whenever there exists a path of arbitrary length.

Exercise 37. *Accordingly to the three steps above to prove $I' \models P(f_{wuz}(\Box), f_{wvz}(\Box))$, build a derivation for the sequent $\vdash$*

$P(f_{wuz}(\Box), f_{wvz}(\Box))$. *Concretely, prove that:*

a. $\varphi' \vdash P(f_z(\Box), f_z(\Box))$, *for* $z \in \Sigma^*$;

b. $\varphi', P(f_z(\Box), f_z(\Box)) \vdash P(f_{uz}(\Box), f_{vz}(\Box))$, *for* $u = v$ *in the set of equations (2.3);*

c. $\varphi', P(f_{uz}(\Box), f_{vz}(\Box)) \vdash P(f_{wuz}(\Box), f_{wvz}(\Box))$, *for* $w \in \Sigma^*$;

d. $\varphi' \vdash P(f_{wuz}(\Box), f_{wvz}(\Box))$.

Comlementary exercise 1. (*) *Continuing exercise 14, the negative fragment of the predicate logic includes all formulas that neither contain disjunctions nor existential quantification and such that all atomic formulas are preceded by negation. Formulas in this fragment have the following syntax.*

$$\phi ::= (\neg p(t, \dots, t)) \;||\; \bot \;||\; (\neg\phi) \;||\; (\phi \wedge \phi) \;||\; (\phi \to \phi) || \; (\forall_x \phi), \quad \textit{for } p \textit{ a predicate symbol and } t \textit{ w-f terms}$$

Prove by induction on ϕ, *that for any formula in the negative fragment of the predicate logic there are derivations in the minimal predicate calculus for*

$$\vdash \phi \leftrightarrow \neg\neg\phi$$

Comlementary exercise 2. (*) *Continuing Exercise 17, consider the negative Gödel translation from predicate logic to intuitionistic predicate logic given by:*

- $\bot^n = \bot$
- $\varphi^n = \neg\neg\varphi$, *if* φ *is an atomic formula.*
- $(\varphi \wedge \psi)^n = \varphi^n \wedge \psi^n$
- $(\varphi \vee \psi)^n = \neg\neg(\varphi^n \vee \psi^n)$

- $(\varphi \to \psi)^n = \varphi^n \to \psi^n$
- $(\forall_x \varphi)^n = \forall_x \varphi^n$
- $(\exists_x \varphi)^n = \neg\forall_x \neg\varphi^n$

Prove that if $\Gamma \vdash \varphi$ *in classical predicate logic then* $\Gamma^n \vdash \varphi^n$ *in intuitionistic predicate logic. Again, since* $\neg\varphi$ *in an abbreviation for* $\varphi \to \bot$, $(\neg\varphi)^n = \neg\varphi^n$.

Chapter 3

Deductions in the Style of Gentzen's Sequent Calculus

Exercise 38.

a. Build a derivation for Modus Tollens; that is, derive the sequent $\varphi \to \psi, \neg\psi \Rightarrow \neg\varphi$.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{(\text{Ax})\ \ \varphi \Rightarrow \varphi \qquad\qquad \psi \Rightarrow \psi\ \ (\text{Ax})}{\varphi \to \psi, \varphi \Rightarrow \psi}\,(\text{L}_{\to}) \qquad\qquad \bot, \varphi \to \psi, \varphi \Rightarrow\ \ (\text{L}_{\bot})}{\varphi \to \psi, \neg\psi, \varphi \Rightarrow}\,(\text{L}_{\to})}{\varphi \to \psi, \neg\psi, \varphi \Rightarrow \bot}\,(\text{RW})}{\varphi \to \psi, \neg\psi \Rightarrow \neg\varphi}\,(\text{R}_{\to})}{}
$$

b. Build derivations for the contraposition rules, (CP_1) *and* (CP_2)*; that is, for the sequents* $\varphi \to \psi \Rightarrow \neg\psi \to \neg\varphi$ *and* $\neg\psi \to \neg\varphi \Rightarrow \varphi \to \psi$.

For (CP_1) *one needs an additional application of the rule* $(\mathrm{R}_\to)$ *to the conclusion of the previous derivation:*

$$\frac{\varphi \to \psi, \neg\psi \Rightarrow \neg\varphi}{\varphi \to \psi \Rightarrow \neg\psi \to \neg\varphi}\,(\mathrm{R}_\to)$$

For (CP_2) *observe the following derivation.*

$$\frac{\dfrac{\dfrac{(\mathrm{Ax})\;\; \varphi, \psi \Rightarrow \psi, \bot}{\varphi \Rightarrow \psi, \neg\psi}\,(\mathrm{R}_\to) \qquad \dfrac{\varphi \Rightarrow \psi, \varphi \;\;(\mathrm{Ax}) \qquad \bot, \varphi \Rightarrow \psi \;\;(\mathrm{L}_\bot)}{\neg\varphi, \varphi \Rightarrow \psi}\,(\mathrm{L}_\to)}{\neg\psi \to \neg\varphi, \varphi \Rightarrow \psi}\,(\mathrm{L}_\to)}{\neg\psi \to \neg\varphi \Rightarrow \varphi \to \psi}\,(\mathrm{R}_\to)$$

c. Build derivations for the contraposition rules, (CP_3) *and* (CP_4).

Exercise 39. (∗) *Prove that weakening rules are unnecessary. It should be proved that all derivations in the sequent calculus can be transformed into a derivation without applications of weakening rules.*

Hint: for doing this you will need to apply induction on the derivations analyzing the case of application of each of the rules just before a last step of weakening. For instance, consider the case of a derivation that finishes in an application of the rule

(LW) *after an application of the rule* ($L_{\rightarrow}$)*:*

$$\dfrac{\dfrac{\begin{array}{c}\nabla_1\\ \Gamma \Rightarrow \Delta, \varphi\end{array} \qquad \begin{array}{c}\nabla_2\\ \psi, \Gamma \Rightarrow \Delta\end{array}}{\varphi \rightarrow \psi, \Gamma \Rightarrow \Delta}\,(L_{\rightarrow})}{\delta, \varphi \rightarrow \psi, \Gamma \Rightarrow \Delta}\,(LW)$$

Thus, a new derivation in which rules (LW) *and* ($L_{\rightarrow}$) *are interchanged can be built as below:*

$$\dfrac{\dfrac{\begin{array}{c}\nabla_1\\ \Gamma \Rightarrow \Delta, \varphi\end{array}}{\delta, \Gamma \Rightarrow \Delta, \varphi}\,(LW) \qquad \dfrac{\begin{array}{c}\nabla_2\\ \psi, \Gamma \Rightarrow \Delta\end{array}}{\psi, \delta, \Gamma \Rightarrow \Delta}\,(LW)}{\delta, \varphi \rightarrow \psi, \Gamma \Rightarrow \Delta}\,(L_{\rightarrow})$$

Then, by induction hypothesis one can assume the existence of derivations without applications of weakening rules, say ∇'_1 *and* ∇'_2*, for the sequents* $\delta, \Gamma \Rightarrow \Delta, \varphi$ *and* $\psi, \delta, \Gamma \Rightarrow \Delta$*, respectively. Therefore a derivation without application of weakening rules of the form below would be possible.*

$$\dfrac{\begin{array}{c}\nabla'_1\\ \delta, \Gamma \Rightarrow \Delta, \varphi\end{array} \qquad \begin{array}{c}\nabla'_2\\ \psi, \delta, \Gamma \Rightarrow \Delta\end{array}}{\delta, \varphi \rightarrow \psi, \Gamma \Rightarrow \Delta}\,(L_{\rightarrow})$$

An additional detail should be taken in consideration in the application of the induction hypothesis: since other possible applications of weakening rules might appear in the derivations ∇_1 *and* ∇_2*, the correct procedure is starting the elimination of* *weakening rules from nodes in the proof-tree in which a first application of a weakening rule is done.*

Indeed, this result requires additional effort. We suggest the reader review the related references given in the Chapter on suggested reading.

Exercise 40.

a. Complete the derivation of the sequent for LEM: $\Rightarrow \varphi \vee \neg\varphi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi, \bot \quad (\mathrm{Ax})}{\Rightarrow \varphi, \neg\varphi}\,(\mathrm{R}_{\to})}{\Rightarrow \varphi \vee \neg\varphi, \neg\varphi}\,(\mathrm{R}_{\vee})}{\Rightarrow \varphi \vee \neg\varphi, \varphi \vee \neg\varphi}\,(\mathrm{R}_{\vee})}{\Rightarrow \varphi \vee \neg\varphi}\,(\mathrm{RC})$$

b. Build a derivation for the sequent $\Rightarrow \neg\neg(\varphi \vee \neg\varphi)$ *using neither rule* (Cut) *nor rule* (RC).

Exercise 41. *(Cf. Exercise 40) Build a minimal derivation in the sequent calculus for the sequent* $\Rightarrow \neg\neg(\varphi \vee \neg\varphi)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\varphi \Rightarrow \varphi \quad (\mathrm{Ax})}{\varphi \Rightarrow \varphi \vee \neg\varphi}\,(\mathrm{R}_{\vee}) \qquad \bot, \varphi \Rightarrow \bot \quad (\mathrm{L}_{\bot})}{\neg(\varphi \vee \neg\varphi), \varphi \Rightarrow \bot}\,(\mathrm{L}_{\rightarrow})}{\neg(\varphi \vee \neg\varphi) \Rightarrow \neg\varphi}\,(\mathrm{R}_{\rightarrow})}{\neg(\varphi \vee \neg\varphi) \Rightarrow \varphi \vee \neg\varphi}\,(\mathrm{R}_{\vee}) \qquad \bot, \neg(\varphi \vee \neg\varphi) \Rightarrow \bot \quad (\mathrm{L}_{\bot})}{\dfrac{\dfrac{\neg(\varphi \vee \neg\varphi), \neg(\varphi \vee \neg\varphi) \Rightarrow \bot}{\neg(\varphi \vee \neg\varphi) \Rightarrow \bot}\,(\mathrm{LC})}{\Rightarrow \neg\neg(\varphi \vee \neg\varphi)}\,(\mathrm{R}_{\rightarrow})}\,(\mathrm{L}_{\rightarrow})$$

Exercise 42 (Cf. Exercise 38)**.** *Give either intuitionistic or classical proofs à la Gentzen for all Gentzen's versions of* (CP) *according to your answers to Exercises 9 and 10.*

a. $\varphi \rightarrow \psi \Rightarrow \neg\psi \rightarrow \neg\varphi$ (CP_1)*;*

b. $\neg\varphi \rightarrow \neg\psi \Rightarrow \psi \rightarrow \varphi$ (CP_2)*;*

c. $\neg\varphi \rightarrow \psi \Rightarrow \neg\psi \rightarrow \varphi$ (CP_3)*; and*

d. $\varphi \rightarrow \neg\psi \Rightarrow \psi \rightarrow \neg\varphi$ (CP_4)*.*

Exercise 43 (Cf. Exercise 38)**.** *Also, provide intuitionistic or classical derivations for the versions below of Modus Tollens, according to your classification in Exercise 11.*

a. $\varphi \rightarrow \psi, \neg\psi \Rightarrow \neg\varphi$ (MT_1)*;*

b. $\varphi \to \neg\psi, \psi \Rightarrow \neg\varphi$ (MT_2);

c. $\neg\varphi \to \psi, \neg\psi \Rightarrow \varphi$ (MT_3); *and*

d. $\neg\varphi \to \neg\psi, \psi \Rightarrow \neg\varphi$ (MT_4).

Exercise 44.

1. *Build an intuitionistic derivation for the sequent* $\Rightarrow \neg\neg(\neg\neg\varphi \to \varphi)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\varphi, \neg\neg\varphi \Rightarrow \varphi \ (\mathrm{Ax})}{\varphi \Rightarrow \neg\neg\varphi \to \varphi}(\mathrm{R}_{\to}) \quad \bot \Rightarrow \bot \ (\mathrm{Ax})}{\neg(\neg\neg\varphi \to \varphi), \varphi \Rightarrow \bot}(\mathrm{L}_{\to})}{\neg(\neg\neg\varphi \to \varphi) \Rightarrow \neg\varphi}(\mathrm{R}_{\to}) \quad \bot \Rightarrow \ (\mathrm{L}_{\bot})}{\neg(\neg\neg\varphi \to \varphi), \neg\neg\varphi \Rightarrow}(\mathrm{L}_{\to})}{\neg(\neg\neg\varphi \to \varphi), \neg\neg\varphi \Rightarrow \varphi}(\mathrm{RW})}{\neg(\neg\neg\varphi \to \varphi) \Rightarrow \neg\neg\varphi \to \varphi}(\mathrm{R}_{\to}) \quad \bot \Rightarrow \bot \ (\mathrm{Ax})}{\neg(\neg\neg\varphi \to \varphi), \neg(\neg\neg\varphi \to \varphi) \Rightarrow \bot}(\mathrm{L}_{\to})}{\neg(\neg\neg\varphi \to \varphi) \Rightarrow \bot}(\mathrm{LC})}{\Rightarrow \neg\neg(\neg\neg\varphi \to \varphi)}(\mathrm{R}_{\to})$$

2. *Build a non classical derivation for the double negation of Peirce's law:* $\Rightarrow \neg\neg(((\varphi \to \psi) \to \varphi) \to \varphi)$.

Exercise 45 (Cf. Exercise 12)**.** *Using the intuitionistic Gentzen's calculus build derivations for the following sequents.*

a. $\neg\neg\neg\phi \Rightarrow \neg\phi$ *and* $\neg\phi \Rightarrow \neg\neg\neg\phi$

b. $\neg\neg(\phi \to \psi) \Rightarrow (\neg\neg\phi \to \neg\neg\psi)$.

c. $\neg\neg(\phi \wedge \psi) \Rightarrow (\neg\neg\phi \wedge \neg\neg\psi)$.

d. $\neg(\phi \vee \psi) \Rightarrow (\neg\phi \wedge \neg\psi)$ *and* $(\neg\phi \wedge \neg\psi) \Rightarrow \neg(\phi \vee \psi)$.

Exercise 46. *Prove all remaining cases in the proof of sufficiency of Theorem 13.*

Exercise 47. *Complete the proof of the Corollary 3.*

Exercise 48. *Complete all details of the proof of Lemma 9.*

For the next exercises, we suggest the reader review the related references given in the Chapter on suggested reading.

Exercise 49. *Prove the remaining cases of the proof of Lemma 10.*

Exercise 50. *Prove all details of Theorem 14.*

Chapter 4

Derivations and Formalizations

The reader will find several PVS theories in the web page of the book of formalization in PVS of simple algebraic examples as gcd, abstract reduction systems and simple sorting algorithms.

Indeed, PVS is given as an option, but not as an obligation and developing such a kind of simple exercises in other proof assistants would be also relevant to be convinced of the usefulness of logic in CS.

Exercise 51. *Consider the PVS specification for* gcd *below (cf. algorithm 2,* gcd_2*, in the introduction). This specification of* gcd *maintains the greatest non null parameter as second argument in the recursive calls by switching the parameters.*

gcd_{sw}*(m : posnat, n : nat) :* **recursive** *nat =*

if $n = 0$ **then**
  m
else
  if $m > n$ **then**
    $gcd_{sw}(n, m)$
  else
    $gcd_{sw}(m, n - m)$
  endif
endif
measure `lex2`(m, n)

Algorithm 4: Specification of gcd with parameter switching in PVS

In first place, specify and prove the TCCs related with type preservation for this specification.

In the case of the function gcd*, TCCs that guarantee the preservation of types for the arguments of the recursive calls are generated, for the first and second recursive calls, respectively, as listed below:*

$$\forall(m : \mathbb{N}^{+}, n : \mathbb{N}) : n \neq 0 \wedge m > n \rightarrow n > 0$$

$$\forall(m : \mathbb{N}^{+}, n : \mathbb{N}) : n \neq 0 \wedge m \leq n \rightarrow n - m \geq 0$$

Under the conditions given for the first recursive call, $gcd_{sw}(n, m)$*, that is* $n \neq 0 \wedge m > n$*, the first TCC guarantees that the first argument in this call would be a positive natural, as required by the parameter specification of the specification. For the second recursive call,* $gcd_{sw}(m, n - m)$*, under its conditions, that is* $n \neq 0 \wedge \neg(m > n)$*, it should be proved that the second argument is a natural, that is,* $n - m \geq 0$*.*

In second place, specify and prove termination TCCs, related with the well-definedness of the specified function gcd_{sw}*. Notice that the measure used now is* $(m,n) \mapsto \mathtt{lex2}(m,n)$ *instead* $(m,n) \mapsto m+n$*, that was adequate for the previous specification of* gcd*; indeed the latter one does not work for the first (parameter switching) recursive call* $(\neg(m+n > n+m))$*. For the selected measure function* `lex2`*, the ordering is given as the lexicographic ordering on the parameters:*

$$\mathtt{lex2}(x,y) > \mathtt{lex2}(u,v) \;\; \textbf{iff} \;\; x > u \vee (x = u \wedge y > v)$$

Now, specify and prove termination TCCs.

$$\forall (m : \mathbb{N}^+, n : \mathbb{N}) : n \neq 0 \wedge m > n \rightarrow \mathtt{lex2}(m,n) > \mathtt{lex2}(n,m)$$

$$\forall (m : \mathbb{N}^+, n : \mathbb{N}) : n \neq 0 \wedge m \leq n \rightarrow \mathtt{lex2}(m,n) > \mathtt{lex2}(m,n-m)$$

The previous TCCs correspond to the next provable formula:

$$\forall (m : \mathbb{N}^+, n : \mathbb{N}) : n \neq 0 \wedge m > n \rightarrow m > n \vee (m = n \wedge n > m)$$

$$\forall (m : \mathbb{N}^+, n : \mathbb{N}) : n \neq 0 \wedge m \leq n \rightarrow m > m \vee (m = m \wedge n > n-m)$$

Exercise 52. *What is the result of applying the PVS proof command* `(flatten)` *to the objective formulas below?*

1. $(A \wedge B \rightarrow C \vee D) \rightarrow C \vee \neg(A \wedge C))$.

2. $(A \wedge B \rightarrow C \vee D) \rightarrow C \vee (A \wedge C))$.

1. `Q.E.D.`.

2. $[-1]\ (A \wedge B \rightarrow C \vee D)$
   `|---`
   $[1]\ C$
   $[2]\ A \wedge C$

Exercise 53. *Using only the PVS proof commands* `(flatten)` *and* `(split)` *prove Peirce's law. That is, prove the sequent* `|---` $((A \rightarrow B) \rightarrow A) \rightarrow A$.

Indeed, only one application of the command `(prop)` *will close the proof of this sequent since it applies repeatedly logical propositional rules and axioms.*

Apply commands `(flatten)` *to obtain the sequent to the left of the previous example. Then apply* `(split)` *as in the example. The proof is concluded applying the command* `(flatten)` *to the sequent* `|---` $A \rightarrow B, A$.

Exercise 54. *Which PVS commands are necessary to prove the following sequents:*

1. `|---` $\forall_{x:T} : P(x) \leftrightarrow \neg\exists_{x:T} : \neg P(x)$;

2. `|---` $\exists_{x:T} : P(x) \leftrightarrow \neg\forall_{x:T} : \neg P(x)$.

1. *Initially, it is necessary to apply the PVS command* `(split)` *in order to branch into two sequents, according to the semantics of the connective* $\leftrightarrow$: `|---` $\forall_{x:T} : P(x) \rightarrow \neg\exists_{x:T} : \neg P(x)$ *and* `|---` $\neg\exists_{x:T} : \neg P(x) \rightarrow \forall_{x:T} : P(x)$.

   The former sequent is proved as in the previous example, by application of the commands `(skolem)` *and* `(inst)`, *after one application of* `(flatten)`.

   For the latter sequent, after applying `(flatten)`, *one obtains the sequent* `|---` $[1]\ \exists_{x:T} : \neg P(x), [2]\ \forall_{x:T} : P(x)$, *which is proved by application of the command (skolem 2 z) and then (inst 1 z).*

2. *The proof is similar to the previous one: after* `(split)` *and corresponding applications of* `(flatten)` *one obtains the sequents* $[-1]\ \exists_{x:T} : P(x),\ [-2]\ \forall_{x:T} : \neg P(x)$ `|---` *and* `|---` $[1]\ \forall_{x:T} : \neg P(x), [2]\ \exists_{x:T} : P(x)$.

   For the former, adequate applications of `(skolem)` *and* `(inst)`*, that correspond to applications of the Gentzen sequent rules* $(\mathrm{L}_\exists)$ *and* $(\mathrm{L}_\forall)$ *will close the proof.*

   For the latter, applications of `(skolem)` *and* `(inst)` *corresponding to the Gentzen sequent rules* $(\mathrm{R}_\forall)$ *and* $(\mathrm{R}_\exists)$ *respectively, will close the proof.*

Exercise 55.

a. *Prove that the relation* $=$ *is transitive for the Gentzen sequent rules.*

b. *Prove that the relation* $=$ *is symmetric and transitive for the rules in deduction natural.*

Exercise 56. *Verify in PVS that the triangle inequality is concluded by a simple application of* `(grind)`*. Also, complete the formalization of the triangle inequality by application of the PVS command* `(expand)` *to the three occurrences of abs in the target objective and repeatedly application of the command* `(lift-if)` *to lift in these definitions inside the target formula. To conclude you also would need to apply either the command* `(split)` *or* `(prop)` *in order to split the target objective into simpler sub objectives. Applications of* `(assert)` *will also be required to deal with the algebra of inequalities over reals.*

Exercise 57. *Explore the application of the last two studied commands* `(decompose-equality)` *and* `(apply-extensionality)` *to equalities between objects of type* `list`*. As usual, in PVS, a list* l *over the non interpreted type* `T`*, that is* `list[T]`*, might be either empty or a cons, checked as* `null?(`l`)` *and* `cons?(`l`)`*, respectively. Thus, data structure of lists own objects that are empty lists* `null` *or built recursively using any element of type* `T`*, say* a*, and a list, say* l*, as* `cons(`a, l`)`*. The head of a non empty list is computed as* `car(`l`)` *and the tail as* `cdr(`l`)`*. How will you deal with an equation of the form* $l1 = l2$ *between non empty lists?*

Exercise 58. *Specify the sums of the examples given in Section 1.3 and prove the equations using the command* `(induct)`*:*

a. $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$,

b. $\displaystyle\sum_{i=0}^{n} k^i = \frac{k^{n+1}-1}{k-1}$, *for* $k \neq 1$.

Exercise 59. *Complete the proof of this conjecture.*

Exercise 60. *a. Complete the proof and formalize the commutativity of* gcd_{sw}*:*

$$\texttt{|---}\ [1]\ \textbf{forall}\ (m:\ \mathit{posnat}, n:\ \mathit{nat}) : n > 0\ \textbf{implies}\ \mathrm{gcd}_{sw}(m,n) = \mathrm{gcd}_{sw}(n,m)$$

As explained in Sec. 4.1.2, this proof does not require induction.

b. Complete the proof of the conjecture

$$\texttt{|---}\ [1]\ \textbf{forall}\ (m:\ \mathit{posnat}, n:\ \mathit{nat}) : \mathit{divides}(\mathrm{gcd}_{sw}(m,n), m).$$

Chapter 5

Algebraic and Computational Examples

As for the previous chapter, the he reader is invited to study the formalizations provided in the web page of the book.

Exercise 61. *Specify and prove that there exist irrationals such that one of them to the power of the other is rational. In PVS you might assume that* $\sqrt{2}$ *is irrational through an axiom as given below.*

`ax1` **:axiom not** `R?(sqrt(2))`

On the other side $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ *can be proved equal to 2 expanding the operators* ^ *and* `expt`*, that are the operators related with the power operator.*

Exercise 62. *Prove by structural induction the previous two lemmas.*

Exercise 63. *a. In the main derivation above, that is* ∇*, complete the step labelled as "*$(L_=)$ *by omitted definition of* `Permutation?`*".*

Notice that rule $(L_=)$ *is being used with equation* `Perm?`$(l_1, l_2) = \forall y\, \mathtt{O}(l_1, y) = \mathtt{O}(l_2, y)$.

b. Complete the steps in the derivation below used in ∇_2 and ∇'_2.

$$\begin{array}{c} Sq_B(l) \equiv\ \Rightarrow \forall x, y\, \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \\ \vdots \\ \neg x = y \Rightarrow \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \end{array}$$

Consider the derivation ∇ below

$$\dfrac{\nabla' \qquad \dfrac{(\text{Ax})\ \neg x = y \Rightarrow \neg x = y \qquad \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \Rightarrow \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)\ (\text{Ax})}{\neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y), \neg x = y \Rightarrow \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)}\,(\text{L}_{\to})}{\neg x = y \Rightarrow \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)}\,(\text{Cut})$$

where ∇' is given by

$$\dfrac{Sq_B(l) \qquad \dfrac{\dfrac{\neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \Rightarrow \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)\ \ (\text{Ax})}{\forall y\, \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \Rightarrow \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)}\,(\text{L}_\forall)}{\forall x, y\, \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y) \Rightarrow \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)}\,(\text{L}_\forall)}{\Rightarrow \neg x = y \to \mathsf{O}(x \cdot l, y) = \mathsf{O}(l, y)}\,(\text{Cut})$$

Exercise 64.

a. Complete all details of this formalization. For doing this you could also check directly the formalization of correctness of quicksort in the theory for sorting algorithms.

b. Build a derivation à la Gentzen Sequent Calculus for this formalization and compare with the proof steps in item a., correspondingly with the proof steps sketched in Fig. 5.4.

Chapter 6

Suggested Readings

We hope, the interested reader would find in this chapter a *road map* to start research on formal logic and deduction, proof theory, type theory, etc.