The main reference for this course is the book [SU06]. However, we frequently depart from the latter regarding presentation and notation, and also on some technical choices. Other references are given within the text.
Contents

1. Introduction 6

2. Propositional Logic 7
   2.1. Natural Deduction for Intuitionistic Propositional Logic 8
   2.1.1. Semantics with Truth Values 10
   2.1.2. Derivable and Admissible Rules 11
   2.2. Intuitionistic Negation 12
      2.2.1. Basic Classical Laws: Excluded Middle and Elimination of Double Negation 12
      2.2.2. Reductio ad Absurdum and The Law of Peirce 14
   2.3. Classical Propositional Logic 15
   2.4. Minimal Implicational Logic 15
   2.5. A Negative Translation 16
   2.6. Glivenko’s Theorem 18

3. The Untyped Lambda-Calculus 19
   3.1. Introduction 19
   3.2. Syntax 20
      3.2.1. The Terms of the Lambda-Calculus 20
      3.2.2. Examples and Notational Conventions 21
      3.2.3. Free and Bound Variables, Towards Alpha-Conversion 21
      3.2.4. Alpha-Conversion via a Locally Nameless Representation 22
   3.3. Beta-Reduction 24
      3.3.1. Capture-Avoiding Substitution 24
      3.3.2. The Notion of Beta-Reduction 24
      3.3.3. The Relation of Beta-Reduction 25
   3.4. Reductions, Conversions and Confluence 25
      3.4.1. Undecidability of Beta-Conversion 28
      3.4.2. A Further Simple Fact on Confluence 29
      3.4.3. Normalization and Newman’s Lemma 29
   3.5. Confluence of Beta-Reduction 30
      3.5.1. Some Basic Properties 31
      3.5.2. Parallel Nested Beta-Reduction 32
      3.5.3. Proof of Confluence 32
      3.5.4. An Alternative Proof by Complete Developments 33
   3.6. Eta-Conversion and Böhm’s Theorem 33
   3.7. Combinatory Logic 34
      3.7.1. Representation of Beta-Conversion 35

4. Curry-Howard Correspondence for Intuitionistic Propositional Logic 37
   4.1. Introduction 37
## Contents

4.2. The Simply-Typed Lambda-Calculus ................................................... 38
  4.2.1. Syntax ................................................. 38
  4.2.2. Main Properties ......................................... 40
4.3. Curry-Howard Correspondence for Intuitionistic Minimal Implicational
  Logic ........................................................................... 41
  4.3.1. Beta-Reduction and Curry-Howard ................................. 43
4.4. Full Intuitionistic Propositional Logic .............................................. 44
  4.4.1. Intuitionistic Conjunctions and Products ............................ 44
  4.4.2. Intuitionistic Disjunctions and Sums ................................ 45
  4.4.3. A Simply-Typed Lambda-Calculus with Sums and Products .... 46
  4.4.4. Main Properties ........................................... 48
  4.4.5. Curry-Howard Correspondence ..................................... 49

5. Normalization for Simple Types .......................................................... 54
  5.1. Introduction .............................................................................. 54
  5.2. Notational Preliminaries ............................................................ 54
  5.3. A First Normalization Result: The Disjunction Property ............... 55
    5.3.1. Weak Head Reduction ............................................... 55
    5.3.2. Type Interpretations and Adequacy ................................. 56
    5.3.3. Proof of the Disjunction Property ................................ 58
  5.4. Reducibility Candidates ............................................................. 60
  5.5. Strong Normalization ............................................................... 62
    5.5.1. Inductive Definition of Strong Normalization .................... 63
    5.5.2. Strong Normalization and Weak Head Reduction ................ 64
    5.5.3. Type Interpretations and Adequacy ................................. 65

6. First-Order Predicate Logic ............................................................... 67
  6.1. Preliminaries ............................................................................. 67
    6.1.1. First-Order Signatures .................................................. 67
    6.1.2. The Language of First-Order Predicate Logic ................. 68
    6.1.3. Structures and Models .................................................... 69
  6.2. Natural Deduction for First-Order Predicate Logic ........................ 71
    6.2.1. Structural Properties .................................................... 73
    6.2.2. Soundness and Completeness w.r.t. the Classical Semantics; Theories 73
    6.2.3. Negative Translations .................................................. 75
    6.2.4. Undecidability ............................................................. 76
    6.2.5. The Failure of Glivenko’s Theorem for Full First-Order Logic 77
    6.2.6. Extraction ................................................................. 78
  6.3. Proof-Terms for Intuitionistic First-Order Predicate Logic ............. 79
    6.3.1. Structural Properties .................................................... 82
    6.3.2. Beta-Reduction .......................................................... 82
    6.3.3. The Full System and its Main Properties ......................... 84
  6.4. First-Order Predicate Logic with Equality .................................... 85
    6.4.1. The Language of First-Order Predicate Logic with Equality 86
6.4.2. Deduction for First-Order Predicate Logic with Equality 86
6.4.3. Models of First-Order Predicate Logic with Equality 87
6.4.4. Negative Translations for First-Order Predicate Logic with Equality 88
6.4.5. Proof-Terms for First-Order Predicate Logic with Equality 88
6.4.6. On Term Extraction and Classical Logic 89
6.5. Normalization 90

7. First-Order Arithmetic 92
7.1. Theories of Natural Numbers with Induction 93
7.2. Peano Arithmetic 95
7.2.1. Primitive Recursive Functions 96
7.2.2. Representation of Computable Functions 97
7.2.3. The Language of First-Order Arithmetic 98
7.2.4. The Axioms of First-Order Arithmetic 99
7.2.5. First-Order Peano Arithmetic 100
7.2.6. Representation and Incompleteness 102
7.2.7. A Classical Arithmetic of True Equalities 103
7.3. Heyting Arithmetic 105
7.3.1. Examples and Basic Properties 105
7.3.2. The Quantifier-Free Formulae of $\mathcal{HA}$ 107
7.3.3. Relation to $\mathcal{PA}$ and Extraction 109
7.3.4. Friedman’s Translation 111

8. Gödel’s System $\mathcal{T}$ 115
8.1. Proof-Terms for Induction 115
8.2. Definition and Main Properties 117
8.2.1. Structural Properties 118
8.2.2. Normalization Properties 119
8.2.3. Expressiveness and Representation 120
8.2.4. Arithmetization 122
8.2.5. Strong Normalization 124
8.3. Modified Realizability 126
8.3.1. Proof of Adequacy 129
8.3.2. Extension to Primitive Disjunctions 133
8.3.3. The Theory of Realized Formulae 134
8.3.4. Realizability with Truth 135

9. Polymorphism 136
9.1. Church-Style System $\mathcal{F}$ 137
9.1.1. Definition 138
9.1.2. Structural Properties 138
9.1.3. Examples of Impredicative Codings 139
9.1.4. Main Properties 144
Contents

9.2. Curry-Style System F .................................................. 145
  9.2.1. Erasing from Church-Style to Curry-Style System F .......... 145
  9.2.2. Examples of Polymorphic Typings of Pure Lambda-Terms ...... 146
  9.2.3. Main Properties .................................................. 148

9.3. Strong Normalization ................................................. 149
  9.3.1. Erasing from Church-style to Curry-style System F .......... 150
  9.3.2. Strong Normalization of Curry-Style System F ............... 150
  9.3.3. Reducibility Candidates ....................................... 151
  9.3.4. Adequacy .......................................................... 152

A. Completeness of Classical Propositional Logic ................. 158
  A.1. A Semantically Reversible Sequent Calculus .................. 158
  A.2. Translation to NK₀ ................................................ 159
  A.3. Completeness of NK₀ .............................................. 160
  A.4. Comparison with other (Compactness and) Completeness Statements .. 160
1. Introduction

The objective of this course is to provide some basics of parts of the theory underlying the Coq\(^1\) proof assistant, namely the **Curry-Howard correspondence** between proofs and programs:

\[
\begin{array}{ccc}
\text{Prog. Languages} & \equiv & \text{Logic} \\
\text{Types} & \equiv & \text{Formulae} \\
\text{Programs} & \equiv & \text{Proofs}
\end{array}
\]

The underlying logic of the Coq system, as well as the core of the Curry-Howard correspondence is **intuitionistic** (or **constructive**\(^2\)). Let us try to explain what does this mean. Consider the following simple fact:

**Fact 1.1.** Either \((\pi + e)\) or \((\pi - e)\) is irrational.

**Proof.** Assume toward a contradiction that \((\pi + e)\) and \((\pi - e)\) are both rational. Then \(2\pi = (\pi + e) + (\pi - e)\) is rational, a contradiction. \(\square\)

However, the following questions are open:\(^3\)

- is \((\pi + e)\) irrational?
- is \((\pi - e)\) irrational?

The guiding principles of intuitionistic reasoning are:

- from a proof of a disjunctive statement, say \(A \lor B\), one should be able to extract either a proof of \(A\) or a proof of \(B\); and

- from a proof of a statement of the form \((\forall x \in \mathbb{N})(\exists y \in \mathbb{N})A(x, y)\), one should be able to extract a computable function \(f : \mathbb{N} \to \mathbb{N}\) such that \((\forall x \in \mathbb{N})A(x, f(x))\).

The argument we gave for Fact 1.1 obviously falls short of the first criterion above. This is crucially due to the use of the non-constructive reasoning principle of **reductio ad absurdum** (RAA). Roughly speaking, intuitionistic logic (IL) is defined from classical logic (CL) by

\[
(\text{CL}) = (\text{IL}) + (\text{RAA})
\]

Intuitionistic (or constructive) mathematics emerged progressively from the 19th century, until their principles were formulated by Brouwer in the early 20th century. It is mainly Heyting who (starting from the 30’s) translated Brouwer’s principles in logical terms, thus establishing them as mathematical objects.

Our approach to intuitionistic logic in this course is to insist on **proofs** rather than on **truth** of formulae. In other words, the important mathematical objects are proofs, which

\(^1\)https://coq.inria.fr/
\(^2\)In this course, we use “intuitionistic” as a technical term qualifying some logical systems, while we use the word “constructive” only informally.
2. Propositional Logic

(by the Curry-Howard correspondence) will be (mostly) seen as terms of some typed \(\lambda\)-calculus. To summarize, our first main topic will be to investigate intuitionistic logics and their relations to typed \(\lambda\)-calculi.

Our second main topic will be to compare intuitionistic systems with their classical counterparts. At first sight, intuitionistic systems are blatantly more restrictive than classical ones since they accept less reasoning principles.

However, there are important logical systems and families of statements for which classical logic is no more powerful than intuitionistic logic. This is crucially the case of formulae expressing program termination. Formulae expressing termination are typically formulae of the form \((\forall x \in \mathbb{N})(\exists y \in \mathbb{N})(t(x, y) = 0)\) where \(t(x, y)\) represents some primitive recursive function. The latter are called \(\Pi^0_2\)-formulae. In many important logical systems containing arithmetic, classical reasoning does not prove more \(\Pi^0_2\)-formulae than intuitionistic reasoning. In other words, in such systems one can prove the termination of the same programs with classical and intuitionistic reasonings.

Moreover (and this is one of the main messages of this course), we see intuitionistic systems as being richer than classical ones. Intuitively, discarding (RAA) makes (most) formulae \(A\) not (logically) equivalent to their double-negation \(\neg\neg A\). As a consequence, there are (intuitively) two notions of disjunction in intuitionistic logic:

1. the plain intuitionistic disjunction \((A \lor B)\),
2. the “classical” intuitionistic disjunction \(\neg\neg(A \lor B)\).

For instance, \((A \lor \neg A)\) is in general not intuitionistically provable, but \(\neg\neg(A \lor \neg A)\) is always intuitionistically provable.

Similarly, there are two existential quantifiers in intuitionistic logic: the plain intuitionistic one \((\exists x)A\) and the “classical” one \(\neg\neg(\exists x)A\).

References. The main reference for this course is the book [SU06].

Concerning intuitionistic logic, a good historical account is given in [TvD88a, Chap. 1] (see also the Notes of [SU06, Chap. 2]). As for general technical introductions, besides [SU06, Chap. 2], the textbook [vD04] is very accessible, while [TvD88a, TvD88b] form a more comprehensive account. Other interesting sources include [Bee85, Koh08].

Regarding typed \(\lambda\)-caluli, (besides [SU06]) a good synthetic but general account is [Bar92], while [Pie02] is a gentle but comprehensive reference book from the point of view of programming languages. An important complementary topic to this course is the denotational semantics of programming languages, for which we refer to [AC98].

Beware however that we should consistently follow the notations and technical definitions of none of these sources.

2. Propositional Logic

This §2 loosely follows [SU06, §2] (as well as parts of [SU06, §6]). Additional references are given within the text.
2. Propositional Logic

We consider formulae given by the grammar:

\[
A, B ::= p \mid A \Rightarrow B \mid A \land B \mid A \lor B \mid \top \mid \bot
\]

where \( p \) ranges over some (unspecified) set of atomic propositions.

Note that there is no primitive notion of negation in the above grammar.

**Notation 2.1** (Negation). We write \( \neg A \) for \( A \Rightarrow \bot \).

We follow the same notational conventions as [SU06, 2.1.2].

**Notation 2.2.**

(1) We assume that implication (\( \Rightarrow \)) associates to the right, so that e.g. \( A \Rightarrow B \Rightarrow C \) stands for \( A \Rightarrow (B \Rightarrow C) \) (which is different from \( (A \Rightarrow B) \Rightarrow C \)).

(2) We assume that negation has the highest priority and implication the lowest, so that e.g. \( A \land \neg B \Rightarrow C \) stands for \( (A \land (\neg B)) \Rightarrow C \).

Finally:

**Notation 2.3.** We write \( A \iff B \) for \( (A \Rightarrow B) \land (B \Rightarrow A) \).

2.1. Natural Deduction for Intuitionistic Propositional Logic

A sequent (for intuitionistic natural deduction) is a pair of the form \( \Delta \vdash A \) where \( A \) is a formula and \( \Delta \) is a (possibly empty) list of formulae. In the literature, \( \Delta \) is sometimes called the antecedent of \( \Delta \vdash A \) and \( A \) its succedent. We shall often call \( \Delta \) the context of \( \Delta \vdash A \). The intended meaning of the sequent \( \Delta_1, \ldots, \Delta_n \vdash A \) is \( (\Delta_1 \land \cdots \land \Delta_n) \Rightarrow A \) (see §2.1.1 below).

The system \( \text{NJ}_0 \) of natural deduction for intuitionistic propositional logic is given by the deduction rules of Fig. 1. These rules have the form

\[
\frac{\Delta_1 \vdash A_1 \quad \ldots \quad \Delta_n \vdash A_n}{\Delta \vdash A}
\]

(with possibly \( n = 0 \)). We say that \( \Delta \vdash A \) is the conclusion, while the sequents \( \Delta_1 \vdash A_1, \ldots, \Delta_n \vdash A_n \) are the premises of the rule. The intended meaning of such a rule is that the conclusion holds whenever so do all the premises.

A derivation in \( \text{NJ}_0 \) is a finite ordered tree whose nodes are labeled by sequents and which respects the rules of Fig. 1 in the following sense:

- given a node \( p \) with list of (immediate) children \( p_1, \ldots, p_n \), there is a rule

\[
\frac{\Delta_1 \vdash A_1 \quad \ldots \quad \Delta_n \vdash A_n}{\Delta \vdash A}
\]

such that \( \Delta \vdash A \) labels \( p \) and \( \Delta_i \vdash A_i \) labels \( p_i \) for each \( i = 1, \ldots, n \).
2. Propositional Logic

\[
\begin{align*}
(Ax) & \frac{\Delta \vdash A}{(A \in \Delta)} \\
(\top\mathbf{-}I) & \frac{\Delta \vdash \top}{(\bot\mathbf{-}E) \frac{\Delta \vdash \bot}{\Delta \vdash A} \\
(\Rightarrow\mathbf{-}I) & \frac{\Delta, A \vdash B}{\Delta \vdash A \Rightarrow B} \\
(\Rightarrow\mathbf{-}E) & \frac{\Delta \vdash A \Rightarrow B}{\Delta \vdash B} \\
(\wedge\mathbf{-}I) & \frac{\Delta \vdash A \quad \Delta \vdash B}{\Delta \vdash A \land B} \\
(\wedge\mathbf{-}E_1) & \frac{\Delta \vdash A \land B}{\Delta \vdash A} \\
(\wedge\mathbf{-}E_2) & \frac{\Delta \vdash A \land B}{\Delta \vdash B} \\
(\vee\mathbf{-}I_1) & \frac{\Delta \vdash A}{\Delta \vdash A \lor B} \\
(\vee\mathbf{-}I_2) & \frac{\Delta \vdash B}{\Delta \vdash A \lor B} \\
(\vee\mathbf{-}E) & \frac{\Delta \vdash A \quad \Delta, A \vdash C\quad \Delta, B \vdash C}{\Delta \vdash C}
\end{align*}
\]

Figure 1: Natural Deduction for Intuitionistic Propositional Logic (NJ0).

In particular, the leaves of a derivation must be labeled by sequents which are instances of rules with no premise.

**Example 2.4.** The following are derivations in NJ0.

1. \( A \vdash A \), using the \((Ax)\)-rule \( \overline{A} \vdash A \).

2. \( A \land B \vdash B \), with the derivation tree

\[
\begin{array}{c}
A \land B \\
\hline
A \land B \vdash A \land B \\
A \land B \vdash A
\end{array}
\]

3. \( A \Rightarrow B, B \Rightarrow C \vdash A \Rightarrow C \), with the derivation tree

\[
\begin{array}{c}
A \Rightarrow B, B \Rightarrow C, A \Rightarrow B, A \vdash B \\
A \Rightarrow B, B \Rightarrow C, A \vdash A \\
A \Rightarrow B, B \Rightarrow C, A \vdash C
\end{array}
\]

**Exercise 2.5.** Show that the following are derivable in NJ0:

1. \( A \land (B \lor C) \vdash (A \land B) \lor (A \land C) \)

2. \( (A \land B) \lor (A \land C) \vdash A \land (B \lor C) \)

The following basic properties are proved by induction on derivations.

**Lemma 2.6** (Structural Rules). The following properties hold in NJ0:
2. Propositional Logic

(weakening) if \( \Delta \vdash A \) then \( \Delta, B \vdash A \);

(contraction) if \( \Delta, B, B \vdash A \) then \( \Delta, B \vdash A \);

(exchange) if \( \Delta, B, \Delta', C, \Delta'' \vdash A \) then \( \Delta, C, \Delta', B, \Delta'' \vdash A \).

Lemma 2.7 (Substitution). In \( \text{NJ}_0 \), if \( \Delta \vdash A \) then \( \Delta[B/p] \vdash A[B/p] \).

Remark 2.8. In the following we shall informally speak of “intuitionistic propositional” logic for the deduction system \( \text{NJ}_0 \). We insist on the fact that there are different possible deduction systems for intuitionistic propositional logic (e.g. sequent calculus, Hilbert systems etc.), while natural deduction systems exist for other logics (classical, linear etc.). We refer to [SU06, §2, §5 & §6]. See also [TvD88a, Chap. 2] as well as [Bus98a, GLT89].

The characteristic property of intuitionistic (propositional) logic is the following.

Theorem 2.9. In intuitionistic propositional logic (\( \text{NJ}_0 \)),

(1) \( \vdash \bot \) is not derivable;

(2) if \( \vdash A \lor B \) then either \( \vdash A \) or \( \vdash B \);

(3) \( \vdash p \lor \neg p \) is not derivable (where \( p \) is an atomic proposition).

Theorem 2.9.(2) is often called the Disjunction Property. We admit it until §4.4.5 (actually §5.3). On the other hand, item (3) (assuming item (2)) as well as item (1) are fairly easy (see §2.1.1 below).

2.1.1. Semantics with Truth Values

Intuitionistic propositional logic is sound w.r.t. the classical semantics.

Definition 2.10 (Classical Semantics).

(1) A valuation \( v \) is a set of atomic propositions.

(2) We define the relation \( v \models A \) (read “\( v \) is a model of \( A \)” or “\( A \) is valid under \( v \)”)

by induction on \( A \) as follows:

\[
\begin{align*}
& v \models p \quad \text{iff} \quad p \in v \\
& v \models A \Rightarrow B \quad \text{iff} \quad (v \models A \implies v \models B) \\
& v \models A \land B \quad \text{iff} \quad (v \models A \land v \models B) \\
& v \models A \lor B \quad \text{iff} \quad (v \models A \lor v \models B) \\
& v \models \top \\
& v \not\models \bot
\end{align*}
\]

(3) A formula \( A \) is valid when \( A \) is valid under all valuations.

(4) A sequent \( A_1, \ldots, A_n \vdash A \) is valid if the formula \( (A_1 \land \cdots \land A_n) \Rightarrow A \) is valid.
2. Propositional Logic

**Remark 2.11** (Soundness w.r.t. Classical Semantics). *It is easy to see that if $\mathbf{NJ}_0$ proves $\Delta \vdash A$ then $\Delta \vdash A$ is valid.*

Beware that the converse of Rem. 2.11 fails: the formula $p \lor \neg p$ is valid but is not provable in $\mathbf{NJ}_0$ (Thm. 2.9.(3)). See §2.3 for the case of classical logic.

Intuitionistic (propositional) logic is complete only w.r.t. weaker notions of validity, relying on stronger semantics (see [SU06, §2.4 & 2.5], also [vD04, TvD88a, TvD88b]). Such semantics in particular give the disjunction property (Thm. 2.9.(2)) without relying on the Curry-Howard correspondence (in contrast with our approach in §4.4), see [SU06, Prop. 2.5.9] (see also [vD04, Thm. 5.4.2]).

**Remark 2.12.** *Soundness w.r.t. classical semantics (Rem. 2.11) trivially gives item (1) of Thm. 2.9. It also easily gives item (3) assuming item (2).*

**Proof.** Assume that $\vdash p \lor \neg p$ is derivable in $\mathbf{NJ}_0$. Then Thm. 2.9.(2) implies that either $\vdash p$ or $\vdash \neg p$ is derivable in $\mathbf{NJ}_0$. But this is a contradiction since neither $p$ nor $\neg p$ is valid in the classical semantics. \qed

A result which is typically proved using (specific) truth values for intuitionistic propositional logic is the decidability of provability in $\mathbf{NJ}_0$. See [SU06, Thm. 2.4.12] (also [vD04, Ex. 15]).

**Theorem 2.13.** *Provability in $\mathbf{NJ}_0$ is decidable.*

### 2.1.2. Derivable and Admissible Rules

We say that a rule

$$
\frac{\Delta_1 \vdash A_1 \quad \ldots \quad \Delta_n \vdash A_n}{\Delta \vdash A}
$$

is **derivable** in a given system (say $\mathbf{NJ}_0$) if there exists a (partial) derivation of $\Delta \vdash A$ in which leaves among $\Delta_1 \vdash A_1, \ldots, \Delta_n \vdash A_n$ are allowed.

A rule as above is **admissible** if its conclusion is derivable whenever all its premises are derivable.

**Example 2.14 (Cut Rule).** *The rule*

$$(\text{Cut}) \quad \frac{\Delta \vdash A \quad \Delta, A \vdash B}{\Delta \vdash B}$$

*is derivable as*

$$
\frac{\Delta \vdash B}{\Delta \vdash A \Rightarrow B} \quad \frac{\Delta \vdash B}{\Delta \vdash A}
$$

**Remark 2.15.** In the following, we use instances of Lem. 2.6 and of Ex. 2.14 without explicit reference.
2. Propositional Logic

2.2. Intuitionistic Negation

Intuitionistic negation is an interesting connective, in particular because in general $\text{NJ}_0$ does not prove $\neg\neg A \vdash A$ (where $\neg A$ is defined in Notation 2.1).

Remark 2.16. In the following (and in accordance with e.g. [TvD88a, Chap. 2, §3]), we record which properties use the (EXFalso) rule (denoted $(\bot\text{-}E)$ in Fig. 1). Note that removing (EXFalso) from $\text{NJ}_0$ results in having no rule for $\bot$.

Intuitionistic logic without (EXFalso) is called minimal logic ([SU06, 2.2.2], see also [TvD88a, Chap. 2, Def. 3.2]). The implicational fragment of minimal logic is discussed in §2.4.

The following gathers simple basic but important properties of intuitionistic negation.

Lemma 2.17. The following are derivable in $\text{NJ}_0$ (without (EXFalso)):

1. $B \Rightarrow \neg A \vdash A \Rightarrow \neg B$
2. $A \vdash \neg\neg A$
3. $A \Rightarrow B \vdash \neg B \Rightarrow \neg A$
4. $A \Rightarrow B \vdash \neg\neg A \Rightarrow \neg B$
5. $\neg\neg\neg A \vdash \neg A$

Proof. Exercise!

Remark 2.18. In the following, we shall often refer to Lem. 2.17 for its combination with Rem. 2.15 (§2.1.2), for instance resulting in the admissible rule

$$\Delta, A \vdash B \quad \Delta, \neg\neg A \vdash \neg\neg B$$

obtained as

$$\Delta \vdash (A \Rightarrow B) \Rightarrow (\neg\neg A \Rightarrow \neg\neg B) \quad \Delta, A \vdash B \quad \Delta \vdash A \Rightarrow B$$

$$\Delta \vdash \neg\neg A \Rightarrow \neg\neg B \quad \Delta, A \vdash B \quad \Delta \vdash \neg\neg A \Rightarrow \neg\neg B$$

$$\Delta, \neg\neg A \vdash \neg\neg A \Rightarrow \neg\neg B$$

2.2.1. Basic Classical Laws: Excluded Middle and Elimination of Double Negation

We now discuss the extension of $\text{NJ}_0$ with some classical principles. This §2.2.1 focuses on the excluded middle and on the elimination of double negation. Reductio ad absurdum (see §1) as well as the more general Peirce’s law are discussed in §2.2.2. In both cases we refer to [SU06, §6.1].
2. Propositional Logic

**Definition 2.19** (Basic Classical Laws).

- The **law of excluded middle** is the rule
  \[ (EM) \quad \Delta \vdash A \lor \neg A \]

- The **double-negation elimination law** is the rule
  \[ (DNE) \quad \Delta \vdash \neg \neg A \Rightarrow A \]

**Lemma 2.20.** \(NJ_0\) (without \((\text{ExFalso})\)) proves \(\vdash \neg \neg (A \lor \neg A)\).

**Proof.** We give the proof tree:

\[
\begin{align*}
\neg (A \lor \neg A) & \vdash \neg (A \lor \neg A) \\
\neg (A \lor \neg A) & \vdash A \\
\neg (A \lor \neg A) & \vdash \bot \\
\neg (A \lor \neg A) & \vdash \neg (A \lor \neg A) \\
\neg (A \lor \neg A) & \vdash A \lor \neg A
\end{align*}
\]

Corollary 2.21. \(NJ_0\) (without \((\text{ExFalso})\) but) augmented with \((\text{DNE})\) proves all instances of \((\text{EM})\).

**Lemma 2.22.** \(NJ_0\) (with \((\text{ExFalso})\) and) augmented with \((\text{EM})\) proves all instances of \((\text{DNE})\).

**Proof.** We give the proof tree:

\[
\begin{align*}
\neg \neg A, \neg A & \vdash \neg A \\
\neg \neg A, \neg A & \vdash A \\
\neg \neg A, \neg A & \vdash \bot \\
\neg \neg A & \vdash \neg \neg A
\end{align*}
\]

Corollary 2.23. The following systems prove the same sequents:

(i) \(NJ_0\) (with \((\text{ExFalso})\) and) augmented with \((\text{DNE})\);

(ii) \(NJ_0\) (with \((\text{ExFalso})\) and) augmented with \((\text{EM})\).

**Remark 2.24** (Non Interdefinability of Connectives). Assuming that there is at least one atomic proposition, in intuitionistic logic connectives are **not** interdefinable as in classical logic. In each case below, there are formulae \(A, B\) such that the indicated sequents are **not** derivable in \(NJ_0\):
2. Propositional Logic

\( (i) \ (A \Rightarrow B) \vdash \neg A \vee B \)

\( (ii) \ \neg(\neg A \land \neg B) \vdash A \lor B \)

\( (iii) \ \neg(\neg A \lor \neg B) \vdash A \land B \)

**Proof.** In each case, we find instances of \( A \) and \( B \) which contradict Thm. 2.9.(3).

(i) We take \( A = B = p \), an atomic proposition. Then \( p \Rightarrow p \) is provable in \( \text{NJ} \) but not \( \neg p \lor p \).

(ii) Assume that \( \text{NJ} \) proves \( \neg(\neg A \land \neg A) \vdash A \lor A \) for all \( A \). Then \( \text{NJ} \) proves all instances of (DNE) (since \( \text{NJ} \) proves \( A \iff (A \land A) \) and \( A \iff (A \lor A) \)), which by Cor. 2.23 implies that \( \text{NJ} \) proves all instances of (EM), a contradiction.

(iii) Similar. \( \square \)

2.2.2. Reductio ad Absurdum and The Law of Peirce

We now complete the investigation of classical principles initiated in §2.2.1. We still refer to [SU06, §6.1].

**Definition 2.25.**

- **The law of Peirce** is the rule

\[
(\text{Peirce}) \quad \Delta \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A
\]

- **The principle of reductio ad absurdum** is the rule

\[
(\text{RAA}) \quad \Delta \vdash (\neg A \Rightarrow A) \Rightarrow A
\]

The principle (RAA) was discussed informally in §1. Its generalization to Peirce’s law is crucial w.r.t. **Minimal Logic** (see §2.4 below).

**Lemma 2.26.** \( \text{NJ} \) (without (EXFALSO) but) augmented with either (EM) or (DNE) proves all instances of (RAA).

**Proof.** Exercise! \( \square \)

**Lemma 2.27.** \( \text{NJ} \) (with (EXFALSO) and) augmented with (RAA) proves all instances of (Peirce), (DNE) and (EM).

**Proof.** Exercise! \( \square \)

**Corollary 2.28.** The following systems prove the same sequents:

(i) \( \text{NJ} \) (with (EXFALSO) and) augmented with (Peirce);
2. Propositional Logic

(ii) \( \text{NJ}_0 \) \((\text{with (ExFalso) and}) \) augmented with (RAA);

(iii) \( \text{NJ}_0 \) \((\text{with (ExFalso) and}) \) augmented with (DNE);

(iv) \( \text{NJ}_0 \) \((\text{with (ExFalso) and}) \) augmented with (EM).

It follows from Thm. 2.9 that the equivalent (w.r.t. provability) systems of Cor. 2.28 are proper extensions of \( \text{NJ}_0 \).

**Remark 2.29.** Note that some instances of seemingly classical principles are actually intuitionistic. We have already seen in Lem. 2.17.(5) that \( \text{NJ}_0 \) admits elimination of double negation over negated formulae. The same is true for (RAA):

- \( \text{NJ}_0 \) \((\text{without (ExFalso)}) \) proves \( \vdash (\neg \neg A \Rightarrow \neg A) \Rightarrow \neg A \).

**Proof.** We give the proof tree:

\[
\begin{align*}
\neg \neg A \Rightarrow \neg A & \vdash \neg \neg A \Rightarrow \neg A & A \vdash \neg \neg A \Rightarrow \neg A \\
\neg \neg A \Rightarrow \neg A, A & \vdash \neg A & \neg \neg A \Rightarrow \neg A, A \vdash A \\
\neg \neg A \Rightarrow \neg A, A & \vdash \bot & \vdash (\neg \neg A \Rightarrow \neg A) \Rightarrow \neg A \\
\end{align*}
\]

\[\square\]

2.3. Classical Propositional Logic

The system \( \text{NK}_0 \) of natural deduction for **classical** propositional logic is \( \text{NJ}_0 \) augmented with the rule (EM). The system \( \text{NK}_0 \) is complete w.r.t. the classical semantics (Def. 2.10, §2.1.1).

**Theorem 2.30** (Completeness of \( \text{NK}_0 \)). \( \text{NK}_0 \) proves all valid sequents.

Theorem 2.30 can be obtained in different ways. We give a proof in Appendix A (Thm A.9, §A.3), which uses a Gentzen-style **sequent calculus** (see [SU06, §7], [GLT89, §5], [Bus98a, §1.2] or [Mel09, §1]).

**Remark 2.31** (Compactness and Related Results). The reader is invited to look at related results (including **compactness**), e.g. [SU06, Thm. 6.1.10] or [Bus98a, Thm. 1.1.3 & Thm. 1.1.5], also [eD04, Thm. 1.5.13]. See §A.4 for a discussion.

2.4. Minimal Implicational Logic

We make a detour via a very simple logic called **minimal implicational logic** (see Rem. 2.16, §2.2). Its formulae are given by the grammar

\[ A, B ::= p \mid A \Rightarrow B \]

where \( p \) ranges over some (unspecified) set of atomic propositions.
2. Propositional Logic

Remark 2.32 (Terminology). Hence minimal implicational logic is the implicational fragment of minimal logic as defined in Rem. 2.16. In the remaining of this §2.4 we write “minimal logic” for “minimal implicational logic”.

Deduction for intuitionistic minimal (implicational) logic is given by the rules of NJ0 restricted to the connectives of minimal logic, namely:

\[(\text{Ax}) \quad \frac{A \in \Delta}{\Delta \vdash A} \quad (\Rightarrow-I) \quad \frac{\Delta, A \vdash B}{\Delta \vdash A \Rightarrow B} \quad (\Rightarrow-E) \quad \frac{\Delta \vdash A \Rightarrow B}{\Delta \vdash B} \quad \frac{\Delta \vdash A}{\Delta \vdash A \Rightarrow B} \]

Note in particular that (ExFalso) is not available, for the reason that there is no \(\bot\) in minimal logic! Also, among the classical principles mentioned in Cor. 2.28, only Peirce’s law is available for minimal logic. We thus define deduction for classical minimal logic to consist of deduction for intuitionistic minimal logic augmented with the rule (Peirce) of Def. 2.25 (§2.2.2):

\[(\text{Peirce}) \quad \frac{\Delta, \Delta \vdash ((A \Rightarrow B) \Rightarrow A)}{\Delta \vdash (A \Rightarrow B) \Rightarrow A} \]

As we shall see in §4.3, minimal logic is the core of the Curry-Howard correspondence. It is also of central importance for Second-Order Logic (see §??).

For the moment we only establish two basic facts about minimal logic.

Proposition 2.33. Assume that there is exactly one atomic proposition. Then classical and intuitionistic minimal logics prove the same sequents.

Proof. Exercise!

Proposition 2.34. Assume that \(p\) and \(q\) are distinct atomic propositions. Then intuitionistic minimal logic does not prove \(\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p\).

Proof. Assume that \(\vdash ((p \Rightarrow q) \Rightarrow p) \Rightarrow p\) is derivable in intuitionistic minimal logic. Then it is also derivable in NJ0, and by the Substitution Lemma 2.7, we get that all instances of (Peirce) are derivable in NJ0. But then Cor. 2.28 implies that NJ0 proves all instances of (EM), which contradicts Thm. 2.9.

Remark 2.35. Note that the proof of Prop. 2.34 apparently uses the classical (RAA). But it is actually intuitionistic since we are proving a negated statement (see Rem. 2.29).

Remark 2.36. One can show that NJ0 is conservative over intuitionistic minimal implicational logic ([SU06, Thm. 2.6.2]), so that the decidability of provability in NJ0 (Thm. 2.13, §2.1.1) implies the decidability of provability in intuitionistic minimal implicational logic.

2.5. A Negative Translation

There are many translations of classical logic to intuitionistic logic in the literature. We study here one such translation, which is a variant of the Gödel-Gentzen translation, see [TvD88a, Chap. 2, §3.4–8]. See also [vD04, Def. 5.2.7], [SU06, §6.4] or [Koh08, §10.1].
2. Propositional Logic

**Definition 2.37** (Negative Translation). The formula $A^\neg$ is defined by induction on $A$ as follows:

1. $p^\neg := \neg\neg p$
2. $\top^\neg := \top$
3. $\bot^\neg := \bot$
4. $(A \Rightarrow B)^\neg := A^\neg \Rightarrow B^\neg$
5. $(A \land B)^\neg := A^\neg \land B^\neg$
6. $(A \lor B)^\neg := \neg(\neg(A^\neg \lor B^\neg))$

**Lemma 2.38.** For each formula $A$, $\text{NJ}_0$ proves $\neg\neg A^\neg \vdash A^\neg$.

**Proof.** Exercise!

**Theorem 2.39.** If $A_1, \ldots, A_n \vdash A$ is derivable in $\text{NK}_0$, then $A_1^\neg, \ldots, A_n^\neg \vdash A^\neg$ is derivable in $\text{NJ}_0$.

**Proof.** Exercise!

**Corollary 2.40.** If $\text{NK}_0$ proves $\vdash A$ then $\text{NJ}_0$ proves $\vdash A^\neg$.

**Remark 2.41** (On Minimal Logic). Corollary 2.40 (i.e. Thm. 2.39) can be strengthened to minimal logic (Rem. 2.16), in the sense that if $\vdash A$ in $\text{NK}_0$ then $\vdash A^\neg$ can be derived in $\text{NJ}_0$ without (ExFalso). To this end, it suffices to observe that the statement of Lem. 2.38 actually holds in minimal logic and that $\bot \vdash A^\neg$ is provable in minimal logic for each formula $A$. We refer to [TvD88a, Chap. 2, §3] for details.

**Remark 2.42.** As we shall see in §6.2.3 and §7.3.4, the translation $(\neg)^\neg$ generalizes to stronger systems, and can be extended so as to provide extraction results (in the sense outlined in §1).

Further, under the Curry-Howard correspondence, variants of $(\neg)^\neg$ extend to continuation-passing style (CPS) translations for (extensions of) the $\lambda$-calculus. For more on this, see [SU06, §6] (and also [Kri09] and [Sel01, §5–8]).

**Remark 2.43** (On the Gödel-Gentzen and Kolmogorov Translations). The translation $(\neg)^\neg$ devised in Def. 2.37 makes transparent the case of (EM) (and of (DNE)) via the clause

$$(A \lor B)^\neg := \neg(\neg(A^\neg \lor B^\neg))$$

(and Lem. 2.38), in particular in view of Lem. 2.20 (§2.2.1). In contrast, the original Gödel-Gentzen translation (see e.g. [TvD88a, Chap. 2, Def. 3.4] or [vD04, Def. 5.2.7]) assumes

$$(A \lor B)^\neg := \neg(\neg A^\neg \land \neg B^\neg)$$

This however does not substantially change the proof of Lem. 2.38 and Thm. 2.39.

On the other hand, in view of Rem. 2.42 it is desirable to consider variants of $(\neg)^\neg$ which avoid Lem. 2.38. This is the case for instance of the following Kolmogorov
2. Propositional Logic

**translation** \((-\)\) (see [TvD88a, Chap. 2, 3.7], and also [SU06, §6.4]):

\[
\begin{align*}
p^{\neg\neg} & := \neg\neg p \\
\top^{\neg\neg} & := \neg\neg\top \\
\bot^{\neg\neg} & := \neg\neg\bot \\
(A \Rightarrow B)^{\neg\neg} & := \neg\neg (A^{\neg\neg} \Rightarrow B^{\neg\neg}) \\
(A \land B)^{\neg\neg} & := \neg\neg (A^{\neg\neg} \land B^{\neg\neg}) \\
(A \lor B)^{\neg\neg} & := \neg\neg (A^{\neg\neg} \lor B^{\neg\neg})
\end{align*}
\]

(we differ from [TvD88a, Chap. 2, 3.7] in the case of \(\top\)). The crucial difference (with both variants of \((-\)\)) is that \((-\)\) relies on the uniform proof of \(\neg\neg\neg A \vdash \neg A\) (Lem. 2.17.(5), §2.2) instead of the inductive and (thus) non-uniform derivations of Lem. 2.38.

2.6. Glivenko’s Theorem

We now discuss Glivenko’s Theorem, a well-known result which establishes that

\[\text{NK}_0\] proves \(\vdash A\) if and only if \([\text{NJ}_0]\) proves \(\vdash \neg\neg A\)

(see [SU06, Thm. 2.4.10] (proved by semantic methods), or e.g. [vD04, Thm. 5.2.10]). At first sight, this result may seem to make the negative translation \((-\)\) useless. Beware that the situation is more subtle, chiefly because Glivenko’s Theorem does not extend to (full) first-order logic, but also for reasons discussed in Rem. 2.50 below.

**Lemma 2.44.** \([\text{NJ}_0]\) proves \(\neg\neg A, \neg\neg B \vdash \neg\neg (A \land B)\).

**Proof.** Exercise! \(\square\)

**Lemma 2.45.** \([\text{NJ}_0]\) proves \((\neg\neg A \Rightarrow \neg\neg B) \vdash \neg\neg (A \Rightarrow B)\).

**Proof.** Exercise! \(\square\)

**Lemma 2.46.** \([\text{NJ}_0]\) proves the following:

1. \(\vdash (\neg\neg A \land \neg\neg B) \iff \neg\neg (A \land B)\)
2. \(\vdash (\neg\neg A \Rightarrow \neg\neg B) \iff \neg\neg (A \Rightarrow B)\)
3. \(\vdash \neg\neg (A \lor B) \Rightarrow (\neg\neg A \Rightarrow \neg\neg C) \Rightarrow (\neg\neg B \Rightarrow \neg\neg C) \Rightarrow \neg\neg C\)

**Proof.** Exercise! \(\square\)

**Proposition 2.47.** If \(A_1, \ldots, A_n \vdash A\) in \([\text{NK}_0]\) then \(\neg\neg A_1, \ldots, \neg\neg A_n \vdash \neg\neg A\) in \([\text{NJ}_0]\).

**Proof.** Exercise! \(\square\)

Glivenko’s Theorem is an immediate consequence of Prop. 2.47.

**Theorem 2.48** (Glivenko). \([\text{NK}_0]\) proves \(\vdash A\) if and only if \([\text{NJ}_0]\) proves \(\vdash \neg\neg A\).
3. The Untyped Lambda-Calculus

An interesting consequence of Glivenko’s Theorem 2.48 is that $\text{NK}_0$ and $\text{NJ}_0$ negate the same formulae.

**Corollary 2.49.** $\text{NK}_0$ proves $A \vdash \bot$ if and only if $\text{NJ}_0$ proves $A \vdash \bot$.

**Proof.** Exercise!

**Remark 2.50.** In comparison with negative translations (such as the translation $(-)^\sim$ discussed in §2.5 above), the main limitation of Glivenko’s Theorem 2.48 is that it does not extend to full first-order logic (we shall discuss this point in §6.2.5).

Besides, the transformation of proofs underlying Thm. 2.48 lacks structure to be (as such) directly exploitable under the Curry-Howard correspondence. The reason is that Lem. 2.44 actually admits two canonical proofs which cannot be equated at the level of the $\lambda$-calculus (without loosing the consistency of its equational theory). This phenomenon has been analyzed in [Gir91], which led to a deep analysis of CPS translations (Rem. 2.42). See [Mel17, §5.7] (in French) for more.

3. The Untyped Lambda-Calculus

3.1. Introduction

The $\lambda$-calculus was invented in 1936 by Alonzo Church, originally with the intent to provide a foundational logical framework based on the notion of function. However, the (pure) untyped $\lambda$-calculus turned out to be inconsistent as a logical system, due to the presence of fixpoints. On the other hand, the latter make the untyped $\lambda$-calculus a Turing-complete model of computation, which constitutes the (theoretical) core of functional traits of programming languages. Moreover, suitable restrictions on the formation of $\lambda$-terms (most notably based on types) make it possible to recover (a range of) logically consistent systems.

**References.** An excellent general but synthetic introduction to the (pure) untyped $\lambda$-calculus is [Bar92, §2]. The standard reference book is [Bar84]. Other important presentations are [AC98, Chap. 2] and [Kri93]. On the other hand, we shall hardly go beyond the material covered in [SU06, Chap. 1].

**Idea.** The $\lambda$-calculus can be thought about as a formal system to represent and manipulate functions. For instance, the function

$$f : x \mapsto x + 3$$

is represented by an expression of the form:

$$f := \lambda x. x + 3$$

Instead of $f(4)$, the application of $f$ to the argument 4 is written

$$(\lambda x.x + 3)4$$
3. The Untyped Lambda-Calculus

Function evaluation is performed by a syntactic manipulation of expressions called \( \beta \)-reduction, and which can be formulated as:

- substitution of “bound variables” by actual arguments.

For instance, it is expected that

\[
(\lambda x. x + 3)4 \text{ evaluates to } 4 + 3
\]

This is formally achieved as:

\[
(\lambda x. x + 3)4 \text{ evaluates to } (x + 3)[4/x]
\]

where \((x + 3)[4/x]\) means \((x + 3)\) in which \(x\) is replaced by \(4\).

Moreover, we shall identify the two following expressions, which only differ by renaming of their “bound variables”, and as such are just two different notations for the same object (see §3.2.3 & §3.2.4 for details):

\[
(\lambda x. x + 3) \text{ and } (\lambda y. y + 3)
\]

An important aspect of the (pure) \(\lambda\)-calculus is the following:

- functions and values are manipulated at the same level, in the sense that they belong to the same class of objects.

Finally, in the \(\lambda\)-calculus there are also higher-order functions, i.e. functions which take functions as arguments, for instance

\[
\lambda f.\lambda x. fx3
\]

Informally, the \(\lambda\)-calculus allows for the following form of computations:

\[
(\lambda f.\lambda x. fx3)(\lambda y.\lambda z. y + z) \text{ evaluates to } \lambda x.(\lambda y.\lambda z. y + z) x3 \\
\lambda x. (\lambda y.\lambda z. y + z) x3 \text{ evaluates to } \lambda x.x + 3
\]

(where e.g. \(fx3\) stands for \((fx)3\), see Notation 3.2 in §3.2 below).

3.2. Syntax

3.2.1. The Terms of the Lambda-Calculus

We assume given a countably infinite set \(X = \{x, y, z, \ldots\}\) of variables. The terms of the \(\lambda\)-calculus (or \(\lambda\)-terms) are given by the grammar

\[
t, u \in \Lambda \ ::= \ x \ | \ \lambda x.t \ | \ tu \quad (\text{where } x \in X)
\]

In the above grammar:

- Terms of the form \(tu\) are called applications. Formally, there is a binary term constructor @, and \(tu\) stands for @\((t, u)\).

- Terms of the form \(\lambda x.t\) are called \(\lambda\)-abstractions. In \(\lambda x.t\), we say that \(\lambda\) is a binder and that \(\lambda x\) is the binding site of \(x\). The variable \(x\) is said to be bound in \(\lambda x.t\).
3. The Untyped Lambda-Calculus

3.2.2. Examples and Notational Conventions

Example 3.1. The following usual λ-terms play an important role in this course:

\[
\begin{align*}
id & := \lambda x.x \\
pair & := \lambda x.\lambda y.\lambda k.(kx)y \\
T & := \lambda x.\lambda y.x \\
F & := \lambda x.\lambda y.y \\
\delta & := \lambda x.xx \\
\Omega & := \delta\delta \\
S & := \lambda n.\lambda x.\lambda y.f(nx)f(y) \\
n & := \lambda x.\lambda f.f(nx) = \lambda x.\lambda f^n x \quad (n \in \mathbb{N})
\end{align*}
\]

The λ-terms \( n \) representing \( n \in \mathbb{N} \) above are called Church’s numerals.

Notation 3.2. The usual notational convention is that application associates to the left, so that \( xyz \) stands for \((xy)z\) (that is \(@(@((x, y), z))\)). With this convention, each λ-term is of the form

\[
\lambda x_1.\ldots.\lambda x_n.yt_1\ldots t_m
\]

or

\[
\lambda x_1.\ldots.\lambda x_n.(\lambda y.u)t_1\ldots t_m
\]

This is called the Wadsworth’s notation.

3.2.3. Free and Bound Variables, Towards Alpha-Conversion

A variable \( x \in \mathcal{X} \) is free in a λ-term \( t \) if it does not occur in the scope of an abstraction \( \lambda x \) in \( t \). This is formalized with the following notion.

Definition 3.3 (Free Variable). The set \( \text{FV}(t) \) of free variables of \( t \) is defined by induction as follows:

\[
\begin{align*}
\text{FV}(x) & := \{ x \} \\
\text{FV}(tu) & := \text{FV}(t) \cup \text{FV}(u) \\
\text{FV}(\lambda x.t) & := \text{FV}(t) \setminus \{ x \}
\end{align*}
\]

Definition 3.4 (Closed Term). A λ-term \( t \) is closed if \( \text{FV}(t) = \emptyset \). We write \( \Lambda_0 \) for the set of closed λ-terms.

On the other hand, the notion of bound variable is much more subtle, because λ-terms are identified up-to (consistent) renaming of their bound variables. Formally, this identification is made via an equivalence relation on \( \Lambda \) called α-equivalence (or α-conversion) and denoted \( =_{\alpha} \). For instance we should have

\[
\lambda y.(\lambda x.xy)(xy) =_{\alpha} \lambda y.(\lambda z.zy)(xy)
\]
3. The Untyped Lambda-Calculus

\[
\begin{align*}
\lambda y. (\lambda x. xy)(xy) & =_\alpha \lambda y. (\lambda y. yy)(xy) \\
\lambda y. (\lambda x. xy)(xy) & =_\alpha \lambda x. (\lambda x.xx)(xx)
\end{align*}
\]

Intuitively, \(\lambda\)-terms quotiented by \(\alpha\)-equivalence can be represented as directed graphs, in which only free variables are named, while bound variables are represented by edges from their occurrences to their binding site. For instance, the \(\alpha\)-equivalence class of \(\lambda y. (\lambda x. xy)(xy)\) could be represented as the graph depicted in Fig. 2 (left). In §3.2.4 we define an algebraic (i.e. term) representation of such graphs.

**Remark 3.5.** A convention which is often adopted in practice, but not always so (easy nor convenient to maintain is Barendregt’s convention, namely:

(i) free and bound variables are always distinct, and

(ii) bound variables are pairwise distinct.

3.2.4. Alpha-Conversion via a Locally Nameless Representation

We define \(\alpha\)-equivalence via an algebraic representation of the graphs such as the one depicted in Fig. 2 (left). This representation uses the well-known de Bruijn indexes to represent bound variables, but still uses names to represent free variables. Such representations are called locally nameless (or sometimes mixed) representations.

The idea of de Bruijn indexes is that an occurrence of a bound variable is represented by a natural number, which counts the number of binders between that occurrence and its binding site. Hence, different occurrences of the same bound variable can be represented by different indexes. For instance, the locally nameless representation of \(\lambda y. (\lambda x. xy)(xy)\) is depicted in Fig. 2 (right).
Formally, we consider the following mixed de Bruijn terms, where \( n \) ranges over natural numbers:

\[
M, N \in \lambda_{DB} ::= \ x \ | \ n \ | \ \lambda M \ | \ MN
\]

The mixed de Bruijn representation of a \( \lambda \)-term \( t \in \Lambda \) is the mixed de Bruijn term \( t^{db} \in \lambda_{DB} \) defined by induction as follows:

\[
x^{db} := x
\]

\[
(\lambda x.t)^{db} := \lambda(t^{db}[x \mapsto 0])
\]

\[
(tu)^{db} := t^{db}u^{db}
\]

where the operation \( M[x \mapsto n] \) is defined by induction as

\[
x[x \mapsto n] := n
\]

\[
y[x \mapsto n] := y \text{ if } y \in X \text{ and } y \neq x
\]

\[
k[x \mapsto n] := k \text{ if } k \in \mathbb{N}
\]

\[
(MN)[x \mapsto n] := (M[x \mapsto n])(N[x \mapsto n])
\]

\[
(\lambda M)[x \mapsto n] := \lambda(M[x \mapsto n + 1])
\]

For instance, we have

\[
(\lambda x.x)^{db} = \lambda((x^{db}[x \mapsto 0])
\]

so that

\[
((\lambda x.x)x)^{db} = (\lambda 0)x
\]

and thus

\[
(\lambda x.(\lambda x.x)x)^{db} = \lambda(((\lambda 0)x[x \mapsto 0])
\]

\[
= \lambda((\lambda 0)0)
\]

Similarly, it is easy to see that in accordance with Fig. 2 (right), we have

\[
(\lambda y.(\lambda x.xy)(xy))^{db} = \lambda((\lambda(01))(x0)) = (\lambda y.(\lambda z.zy)(xy))^{db}
\]

**Definition 3.6 (\( \alpha \)-Equivalence).** Two \( \lambda \)-terms \( t, u \) are \( \alpha \)-equivalent, notation \( t =_\alpha u \), if \( t^{db} = u^{db} \).

**Notation 3.7.** From now on, \( \lambda \)-terms will be always considered up-to \( \alpha \)-equivalence. In particular, we still write \( \Lambda \) for the set \( \Lambda \) quotiented by \( =_\alpha \).

We refer to [Cha12] for further details and references on the locally nameless representation. For other approaches and references see e.g. [SU06, Chap. 1] or [Kri93, Chap. 1].
3.3. Beta-Reduction

Beta-reduction (written $\beta$-reduction) is the core computation mechanism of the $\lambda$-calculus. The basic idea of $\beta$-reduction can be phrased as follows:

- $(\lambda x.t)u$ (read “function $\lambda x.t$ applied to argument $u$”) is evaluated by replacing the formal parameter of the function (the bound variable $x$) by its actual parameter (the argument $u$).

If we informally write

$$t \triangleright_\beta u \quad \text{for} \quad t \text{ evaluates to } u$$

then following are expected behaviours of $\beta$-reduction.

\[
\begin{align*}
id \ id &= (\lambda x.x)id \triangleright_\beta id \\
id \ \delta &= (\lambda x.x)\delta \triangleright_\beta \delta \\
\delta \ id &= (\lambda x.xx)id \triangleright_\beta id \triangleright_\beta id \\
\Omega &= \delta\delta = (\lambda x.xx)\delta \triangleright_\beta \delta\delta \triangleright_\beta ...
\end{align*}
\]

3.3.1. Capture-Avoiding Substitution

The key technical ingredient of $\beta$-reduction is the operation of capture-avoiding substitution.

**Definition 3.8 (Capture-Avoiding Substitution).** The capture-avoiding substitution $t[u/x]$ is defined by induction on $t$ as follows:

\[
\begin{align*}
y[u/x] & := y \quad \text{if } y \neq x \\
x[u/x] & := u \\
(t_1 t_2)[u/x] & := t_1[u/x] t_2[u/x] \\
(\lambda y.t)[u/x] & := \lambda y.t[u/x] \quad \text{if } y \neq x \text{ and } y \notin \text{FV}(u)
\end{align*}
\]

**Remark 3.9.** Capture avoiding substitution is a total operation on $\lambda$-terms quotiented by $\alpha$-equivalence.

3.3.2. The Notion of Beta-Reduction

**Definition 3.10 (Notion of $\beta$-reduction).** The notion of $\beta$-reduction is the relation $\triangleright_\beta$ defined as

$$(\lambda x.t)u \triangleright_\beta t[u/x]$$

Terms of the form $(\lambda x.t)u$ are called $\beta$-redexes.
3. The Untyped Lambda-Calculus

3.3.3. The Relation of Beta-Reduction

The notion of \( \beta \)-reduction is actually too weak, since we may have to reduce \( \beta \)-redexes which are not at top level. Consider for instance the terms:

\[
\text{id}(\lambda xy.yx)(\lambda x.yy) \quad \lambda x.(\lambda x.xx)\text{id} \quad (\lambda x.xx)\text{id}\text{id}
\]

Definition 3.11 (Congruence). Let \( R \) be a binary relation on \( \lambda \)-terms.

1. We say that \( R \) is compatible if it is closed under the rules:

\[
\begin{align*}
  & t R t' \quad u R u' \quad t R t' \\
  & t u R t' u \quad t u R t' u \quad \lambda x. t R \lambda x. t'
\end{align*}
\]

2. We say that \( R \) is a congruence if \( R \) is a compatible equivalence relation.

Definition 3.12 (Full (Strong) \( \beta \)-Reduction). The relation of full (strong) \( \beta \)-reduction (still denoted \( \triangleright_\beta \)) is the least compatible relation such that

\[
(\lambda x.t) u \triangleright_\beta t\left[ u/x \right]
\]

Remark 3.13. Note that \( \alpha \)-conversion may need to be performed on the fly in a sequence of \( \beta \)-reductions:

\[
id(\lambda xy.yx)(\lambda x.yy) \triangleright_\beta (\lambda xz.zx)(\lambda x.yy) \quad =_\alpha \quad \lambda z.\lambda x.yy
\]

Recall that \( \Lambda_0 \) stands for the set of closed \( \lambda \)-terms (Def. 3.4, §3.2.3).

Remark 3.14. Note that \( \Lambda_0 \) is stable under \( \beta \)-reduction: if \( t \in \Lambda_0 \) and \( t \triangleright_\beta u \) then \( u \in \Lambda_0 \).

3.4. Reductions, Conversions and Confluence

Let us look at some possibilities allowed by \( \beta \)-reduction.

Example 3.15. Recall the \( \lambda \)-terms from Ex. 3.1 (§3.2.2).

1. Given \( n \in \mathbb{N} \) we have

\[
n \text{id} \text{id} \triangleright_\beta \text{id} \underbrace{\text{id}(\text{id} \text{id} \ldots)}_{n} \triangleright_\beta^n \text{id}
\]

So we may have to consider many consecutive steps of \( \beta \)-reduction.

2. We have two ways for reducing \( (\text{id} \text{id})(\text{id} \text{id}) \) to \( \text{id} \), namely

\[
(\text{id} \text{id})(\text{id} \text{id}) \triangleright_\beta \text{id}(\text{id} \text{id}) \triangleright_\beta \text{id} \text{id} \triangleright_\beta \text{id}
\]

This gives three ways for reducing \( \delta(\text{id} \text{id}) \) to \( \text{id} \text{id} \):

\[
\delta(\text{id} \text{id}) \triangleright_\beta \text{id}(\text{id} \text{id}) \triangleright_\beta \text{id} \text{id} \triangleright_\beta \text{id} \quad \delta(\text{id} \text{id}) \triangleright_\beta \text{id}(\text{id} \text{id}) \triangleright_\beta \text{id} \text{id} \triangleright_\beta \text{id}
\]

and

\[
\delta(\text{id} \text{id}) \triangleright_\beta \delta \text{id} \triangleright_\beta \text{id} \text{id} \triangleright_\beta \text{id}
\]
Our goal in this §3.4 is to introduce notations for iterated \( \beta \)-reduction and to discuss a simple (but not trivial) property of \( \beta \)-reduction on pure \( \lambda \)-terms, called \textbf{confluence}, which says any two different (finite) iterations of \( \beta \)-reduction from a given \( \lambda \)-term can always be joined by (finite) iterations of \( \beta \)-reduction (see Thm. 3.20 and Def. 3.19 below). On our way we shall note some important well-known facts.

We begin with the following (usual) definitions, for which a good reference is the textbook [BN98].

\textbf{Definition 3.16} (Abstract Reduction System). An \textbf{ARS} \((A, \triangleright)\) is set \(A\) equipped with a binary relation \(\triangleright \subseteq A \times A\).

Let \((A, \triangleright)\) be an ARS.

- The \textbf{transitive closure} of \(\triangleright\), written \(\triangleright^+\), is the least relation closed under the rules:
  
  \[
  \begin{array}{c}
  a \triangleright b \\
  \end{array} \quad \begin{array}{c}
  a \triangleright^+ b \\
  b \triangleright^+ c \\
  a \triangleright^+ c \\
  \end{array}
  \]

- The \textbf{reflexive and transitive closure} of \(\triangleright\), written \(\triangleright^*\), is the least relation closed under the rules:
  
  \[
  \begin{array}{c}
  a \triangleright b \\
  a \triangleright^* b \\
  a \triangleright a \\
  a \triangleright^* a \\
  a \triangleright^* b \\
  b \triangleright^* a \\
  a \triangleright^* c \\
  b \triangleright^* c \\
  \end{array}
  \]

- The \textbf{symmetric, reflexive and transitive closure} of \(\triangleright\), written \(\triangleleft \triangleright^*\), is the least relation closed under the rules:
  
  \[
  \begin{array}{c}
  a \triangleright b \\
  a \triangleleft \triangleright^* b \\
  a \triangleleft \triangleright^* a \\
  a \triangleleft \triangleright^* b \\
  b \triangleleft \triangleright^* a \\
  a \triangleleft \triangleright^* c \\
  b \triangleleft \triangleright^* c \\
  \end{array}
  \]

\textbf{Notation 3.17}. In the case of \(\beta\)-reduction, we write \(t =_\beta u\) for \(t \triangleleft \triangleright^*_\beta u\).

\textbf{Example 3.18}. For instance, we have

\[
\begin{array}{l}
\text{id id} \triangleright^\beta \text{id} \\
\delta \text{id} \triangleright^\beta \text{id} \\
\delta \delta \triangleright^\beta \delta \delta \\
\text{id} \triangleright^\beta \text{id} \\
(\text{id id})\text{id} =_\beta \text{id(id id)}
\end{array}
\]

\textbf{Definition 3.19} (Confluence). Let \((A, \triangleright)\) be an ARS.

- The relation \(\triangleright\) is \textbf{confluent} if whenever \(a \triangleright^* b\) and \(a \triangleright^* c\), there is \(d \in A\) such that \(b \triangleright^* d\) and \(c \triangleright^* d\).
3. The Untyped Lambda-Calculus

• The relation $\triangleright$ is **locally confluent** if whenever
  
  \[
  a \triangleright b \quad \text{and} \quad a \triangleright c
  \]

  there is $d \in A$ such that
  
  \[
  b \triangleright^* d \quad \text{and} \quad c \triangleright^* d
  \]

• The relation $\triangleright$ has the **diamond property** if whenever
  
  \[
  a \triangleright b \quad \text{and} \quad a \triangleright c
  \]

  there is $d \in A$ such that
  
  \[
  b \triangleright d \quad \text{and} \quad c \triangleright d
  \]

We can now state Thm. 3.20.

**Theorem 3.20** (Confluence of $\beta$-reduction). The relation $\triangleright_\beta$ is confluent.

We shall prove Thm. 3.20 in §3.5.

A important consequence of Thm. 3.20 is that the equational theory $=_{\beta}$ is consistent, in the sense that there terms $t, u$ such that $t \not=_{\beta} u$. This is given by the following simple and well-known property. See e.g. [BN98, Thm. 2.1.5] for a proof.

**Proposition 3.21** (Church-Rosser and Confluence). Let $(A, \triangleright)$ be an ARS. Then $\triangleright$ is confluent if and only if whenever

\[
    a \quad <\triangleright^* \quad b
\]

there is $c \in A$ such that

\[
    a \triangleright^* c \quad \text{and} \quad b \triangleright^* c
\]

**Corollary 3.22.** The equational theory $=_{\beta}$ is consistent.

**Proof.** Recall from Ex. 3.1 (§3.2.2) the terms $T$ and $F$. We claim that $T \not=_{\beta} F$. Indeed, if $T =_{\beta} F$ then by Prop. 3.21 and Thm. 3.20 there would be a $\lambda$-term $t$ such that $T \triangleright^*_\beta t$ and $F \triangleright^*_\beta t$. But this is impossible since $T$ and $F$ are distinct $\lambda$-terms which cannot be $\beta$-reduced.

**Remark 3.23.** Note that if $\mathcal{R}$ is congruence (Def. 3.11, §3.3.3) which contains $=_{\beta}$ and such that $T \mathrel{\mathcal{R}} F$, then we have $t \mathrel{\mathcal{R}} u$ for all $\lambda$-terms $t, u$.

**Proof.** Exercise!
3. The Untyped Lambda-Calculus

3.4.1. Undecidability of Beta-Conversion

We mention here some important well-known results on the undecidability of \( \beta \)-conversion for the (pure) untyped \( \lambda \)-calculus. Recall that \( \Lambda_0 \) stands for the set of closed \( \lambda \)-terms (Def. 3.4, §3.2.3).

**Definition 3.24.** The relation of **closed** \( \beta \)-conversion \( \equiv_{\beta_0} \) is the symmetric reflexive transitive closure of \((\Lambda_0, \rightarrow_{\beta})\).

Note that it follows from the confluence of \( \beta \)-reduction (Thm. 3.20) together with Prop. 3.21 and Rem. 3.14 (§3.3) that given closed \( \lambda \)-terms \( t, u \in \Lambda_0 \), if \( t =_{\beta} u \) then \( t =_{\beta_0} u \).

**Definition 3.25.**

1. A **\( \beta \)**-equationally saturated set is a set \( S \subseteq \Lambda \) which is stable under \( \beta \)-conversion (i.e. if \( t \in S \) and \( t =_{\beta} u \) then \( u \in S \)).

   A \( \beta \)-equationally saturated set \( S \) is **non-trivial** if \( S \neq \emptyset \) and \( S \neq \Lambda \).

2. A **\( \beta_0 \)**-equationally saturated set is a set \( S_0 \subseteq \Lambda_0 \) which is stable under \( =_{\beta_0} \).

   A \( \beta_0 \)-equationally saturated set \( S_0 \) is **non-trivial** if \( S_0 \neq \emptyset \) and \( S_0 \neq \Lambda_0 \).

**Theorem 3.26.**

1. If \( S \) is \( \beta \)-equationally saturated and non-trivial then \( S \) is not recursive.

2. If \( S_0 \) is \( \beta_0 \)-equationally saturated and non-trivial then \( S_0 \) is not recursive.

Theorem 3.26.(1) is [Bar92, Thm. 2.2.15] (see also [Bar84, Thm. 6.6.2]), and Thm. 3.26.(2) is [Bar84, Cor. 6.6.4]. Both results follow from the Turing-completeness of the untyped \( \lambda \)-calculus (see e.g. [Bar92, Thm. 2.2.12]) and from manipulation of suitable Gödel numbers (see e.g. [Bar92, §2.2]).

We are interested in Thm. 3.26 for its following corollaries.

**Corollary 3.27.**

1. The set following set of \( \lambda \)-terms is not recursive:

\[
\{ t \in \Lambda \mid t =_{\beta} T \}
\]

2. The set following set of closed \( \lambda \)-terms is not recursive:

\[
\{ t \in \Lambda_0 \mid t =_{\beta_0} T \}
\]

Corollary 3.27 is essentially due to Church (see [Bar84, §6.6] for references). The undecidability of \( \beta \)-conversion is an immediate consequence.

**Corollary 3.28.** The following problems are undecidable:

- Given \( \lambda \)-terms \( t \) and \( u \), decide whether \( t =_{\beta} u \).
- Given closed \( \lambda \)-terms \( t \) and \( u \), decide whether \( t =_{\beta_0} u \).
3. The Untyped Lambda-Calculus

3.4.2. A Further Simple Fact on Confluence

Returning to Def. 3.19, it is not difficult to show that

Diamond Property $\Rightarrow$ Confluence $\Rightarrow$ Local Confluence

We sketch here the proof of the fact that the diamond property implies confluence, since this plays a crucial role in our proof of Thm. 3.20.

**Notation 3.29.** Given an ARS $(A, \triangleright)$ and $n \in \mathbb{N}$, let $a \triangleright^n b$ if there are $c_0, \ldots, c_n \in A$ such that $a = c_0$, $b = c_n$ and $c_i \triangleright c_{i+1}$ for all $i < n$.

**Lemma 3.30.** Let $(A, \triangleright)$ be an ARS. Assume that $\triangleright$ satisfies the diamond property. Let $a, b, c \in A$ and $n, m \in \mathbb{N}$ such that $a \triangleright^n b$ and $a \triangleright^m c$. Then there is some $d \in A$ such that $b \triangleright^m d$ and $c \triangleright^n d$.

**Proof.** Exercise!

The confluence of a relation with the diamond property is then given by the following.

**Lemma 3.31.** Let $(A, \triangleright)$ be an ARS. We have

$$\triangleright^* = \bigcup_{n \in \mathbb{N}} \triangleright^n$$

**Proof.** Exercise!

**Corollary 3.32.** If $(A, \triangleright)$ has the diamond property, then $(A, \triangleright)$ is confluent.

3.4.3. Normalization and Newman’s Lemma

We briefly discuss here a well-known method to prove the confluence of some ARS’s. While this method is not applicable to prove the confluence of the untyped $\lambda$-calculus, it is of some use for typed extensions of the pure $\lambda$-calculus (e.g. §4.4).

**Definition 3.33** (Normal forms and Normalization). Let $(A, \triangleright)$ be an ARS.

- We say that $a \in A$ is a **normal form** if there is no $b \in A$ such that $a \triangleright b$.
- We say that $a \in A$ is **weakly normalizing** if there is a normal form $b \in B$ such that $a \triangleright^* b$. In this case we say that $b$ is a normal form of $a$.
  We say that $\triangleright$ is weakly normalizing if every $a \in A$ is weakly normalizing.
- We say that $a \in A$ is **strongly normalizing** if there is no infinite reduction sequence starting from $a$.
  We say that $\triangleright$ is strongly normalizing if every $a \in A$ is strongly normalizing.

When we just say “normalizing“, we usually mean **weak** rather than **strong** normalization.
3. The Untyped Lambda-Calculus

Example 3.34. For instance, w.r.t. $\beta$-reduction,

- the $\lambda$-terms $\text{id}$ and $(\text{id} \text{id})$ are strongly normalizing,
- the $\lambda$-term $(\delta \delta)$ is not (even weakly) normalizing,
- the $\lambda$-term $(\lambda xy.y)(\delta \delta)$ is not strongly normalizing, but it is weakly normalizing.

A strongly normalizing ARS is confluent whenever it is locally confluent. See e.g. [BN98, Lem. 2.7.2] for a proof.

Lemma 3.35 (Newman). Let $(A, \rightarrow)$ be an ARS. If $\rightarrow$ is locally confluent and strongly normalizing, then $\rightarrow$ is confluent.

Note that (a necessarily not strongly normalizing) $(A, \rightarrow)$ can be locally confluent and (weakly) normalizing without being confluent.

Example 3.36. The ARS $\left(\{a, b, c, d\}, \rightarrow\right)$, where

$$ a \quad b \quad c \quad d $$

is locally confluent, weakly normalizing but not confluent (since $a$ and $d$ are distinct normal forms).

Remark 3.37. Newman’s lemma cannot be applied to prove the confluence of $\rightarrow_\beta$ on untyped $\lambda$-terms, since not every $\lambda$-term is strongly $\beta$-normalizing (e.g. $\Omega \rightarrow_\beta \Omega$).

3.5. Confluence of Beta-Reduction

We now prove Thm. 3.20. We use a technique due to Tait and Martin-Löf (see e.g. [SU06, §1.4]). The main idea is to target a diamond property. Note that $\rightarrow_\beta$ does not have the diamond property since the two one-step $\beta$-reducts of $(\delta (\text{id} \text{id}))$, namely

$$(\text{id} \text{id}) (\text{id} \text{id}) \beta (\delta (\text{id} \text{id})) \beta \delta \text{id}$$

can be joined, but not in one step of $\beta$-reduction.

The trick is to look for a relation $\parallel_\beta$ with the diamond property and such that $\rightarrow_\beta \subseteq \parallel_\beta \subseteq \rightarrow_\beta^*$. The example of $\delta (\text{id} \text{id})$ above suggests to allow for parallel $\beta$-reduction steps in $\parallel_\beta$. Technically, we assume that $\parallel_\beta$ is reflexive, compatible (Def. 3.11, §3.3.3), and closed under the rule

$$
\begin{align*}
  t \parallel_\beta t' & \quad u \parallel_\beta u' \\
  tu & \parallel_\beta t'u'
\end{align*}
$$

We can then close the case of $\delta (\text{id} \text{id})$ above with

$$(\text{id} \text{id})(\text{id} \text{id}) \parallel_\beta \text{id} \text{id}$$

Now, allowing for parallel $\beta$-reduction leads to the following one-step reducts:

$$(\lambda y.(\text{id} \text{id}) (\text{id} \text{id})) \text{id} \beta (\lambda x.((\lambda y.xx)\text{id}) (\text{id} \text{id}) \parallel_\beta \delta \text{id}$$
3. The Untyped Lambda-Calculus

The relation $\triangleright_{\|\beta}$ is further required to allow for the simultaneous reduction of nested $\beta$-redexes, as expressed by the rule

$$
\frac{t \triangleright_{\|\beta} t' \quad u \triangleright_{\|\beta} u'}{(\lambda x.t)u \triangleright_{\|\beta} t'[u'/x]}
$$

We thus have

$$
(\lambda y.(\text{id } \text{id})(\text{id } \text{id}))\text{id} \triangleright_{\|\beta} \text{id } \text{id}
$$

and conclude the example with $\delta \text{id} \triangleright_{\beta} \text{id } \text{id}$.

As we shall see in §3.5.2 below, the above requirements lead to a relation $\triangleright_{\|\beta}$ with the diamond property and such that $\triangleright_{\beta} \subseteq \triangleright_{\|\beta} \subseteq \triangleright_{\tau_{\beta}}$.

3.5.1. Some Basic Properties

We begin with some basic properties of substitution and (usual) $\beta$-reduction. First, a simple property of $\triangleright_{\tau_{\beta}}$.

**Lemma 3.38.** The relation $\triangleright_{\tau_{\beta}}$ is closed under the two following rules

$$
\frac{t \triangleright_{\tau_{\beta}} t' \quad \lambda x.t \triangleright_{\beta} \lambda x.t'}{\lambda x.t \triangleright_{\tau_{\beta}} \lambda x.t'}
\quad
\frac{t \triangleright_{\tau_{\beta}} t' \quad u \triangleright_{\tau_{\beta}} u'}{tu \triangleright_{\tau_{\beta}} t'u'}
$$

**Proof.** Exercise! □

**Remark 3.39.** Otherwise said, $\triangleright_{\tau_{\beta}}$ is a compatible relation (Def. 3.1.1, §3.3.3). We similarly obtain that $=_{\beta}$ is compatible, so that it is actually a congruence.

We now turn to a standard technical property on iterated substitutions. See e.g. [SU06, Lem. 1.2.20] or [Bar92, Lem. 2.3.14].

**Lemma 3.40.** If $x \notin \text{FV}(v)$ and $x \neq y$ then

$$
t[u/x][v/y] = t[v/y][u[v/y]/x]
$$

**Proof.** Exercise! □

The following is an easy property of $\beta$-reduction.

**Lemma 3.41.**

1. If $t \triangleright_{\beta} u$ then $t[v/x] \triangleright_{\beta} u[v/x]$.
2. If $t \triangleright_{\tau_{\beta}} u$ then $t[v/x] \triangleright_{\tau_{\beta}} u[v/x]$ (and similarly for $\triangleright_{\beta}$).
3. If $t \triangleright_{\beta} u$ then $v[t/x] \triangleright_{\tau_{\beta}} v[u/x]$.

**Proof.** Exercise! □
3. The Untyped Lambda-Calculus

3.5.2. Parallel Nested Beta-Reduction

We shall prove Theorem 3.20 using an auxiliary notion of parallel and nested β-reduction.

**Definition 3.42** (Parallel Nested β-Reduction). The relation $\triangleright_{\parallel\beta}$ is the least binary relation on λ-terms which is closed under the following rules

\[
\begin{align*}
x & \triangleright_{\parallel\beta} x & t & \triangleright_{\parallel\beta} t' & u & \triangleright_{\parallel\beta} u' \\
& & tu & \triangleright_{\parallel\beta} tu' & t & \triangleright_{\parallel\beta} t' & u & \triangleright_{\parallel\beta} u' \\
& & t & \triangleright_{\parallel\beta} t' & (\lambda x.t)u & \triangleright_{\parallel\beta} t'[u'/x]
\end{align*}
\]

We begin with some easy basic properties of $\triangleright_{\parallel\beta}$.

**Lemma 3.43.** The relation $\triangleright_{\parallel\beta}$ is reflexive (i.e. $t \triangleright_{\parallel\beta} t$ for all λ-terms $t$).

**Proof.** Exercise! □

**Lemma 3.44.** We have $\triangleright_{\beta} \subseteq \triangleright_{\parallel\beta}$ (i.e. if $t \triangleright_{\beta} u$ then $t \triangleright_{\parallel\beta} u$).

**Proof.** Exercise! □

**Lemma 3.45.** We have $\triangleright_{\parallel\beta} \subseteq \triangleright_{\beta}^*$ (i.e. if $t \triangleright_{\parallel\beta} u$ then $t \triangleright_{\beta}^* u$).

**Proof.** Exercise! □

The key property of $\triangleright_{\parallel\beta}$ is the following.

**Lemma 3.46.** If $t \triangleright_{\parallel\beta} u$ and $v \triangleright_{\parallel\beta} w$ then $t[v/x] \triangleright_{\parallel\beta} u[w/x]$.

**Proof.** Exercise! □

The main interest of $\triangleright_{\parallel\beta}$ is that it satisfies the diamond property.

**Proposition 3.47.** The relation $\triangleright_{\parallel\beta}$ satisfies the diamond property.

**Proof.** Exercise! □

3.5.3. Proof of Confluence

We can finally prove that $\triangleright_{\beta}$ is confluent (Thm. 3.20).

**Proof.** Exercise! □
3. The Untyped Lambda-Calculus

3.5.4. An Alternative Proof by Complete Developments

We briefly discuss here the proof of Prop. 3.47 presented in [SU06] (namely [SU06, Def. 1.4.3 & Lem. 1.4.4]), which relies on the notion of complete development. The idea is to reduce in one step all the β-redexes present in a term.

Definition 3.48. The complete development of $t$, written $t^\bullet$, is inductively defined as:
\[
\begin{align*}
x^\bullet & := x \\
(\lambda x.t)^\bullet & := \lambda x.t^\bullet \\
(tu)^\bullet & := t^\bullet u^\bullet \quad \text{if } t \text{ is not an abstraction} \\
((\lambda x.t)u)^\bullet & := t^\bullet [u^\bullet/x]
\end{align*}
\]

Lemma 3.49. If $t \triangleright_{\beta} v$ then $v \triangleright_{\beta} t^\bullet$.

Proof. Exercise! \hfill \Box

Corollary 3.50. The relation $\triangleright_{\beta}$ satisfies the diamond property.

Proof. Exercise! \hfill \Box

3.6. Eta-Conversion and Böhm’s Theorem

We briefly discuss here a syntactic notion of extensionality for the $\lambda$-calculus. More precisely, we are going to give an equational axiomatization of the relation $\equiv$ on $\lambda$-terms defined as the least equivalence relation closed under the rules
\[
\begin{align*}
t =_\beta u & \quad \quad \frac{t \equiv u}{t } \quad \quad \frac{tx \equiv ux \quad (x \notin \text{FV}(t,u))}{t \equiv t} \\
& \quad \quad \frac{t \equiv t' \quad u \equiv u'}{tu \equiv t'u'}
\end{align*}
\]

The relation $\equiv$ can be axiomatized as the least congruence (Def. 3.11, §3.3.3) containing $\beta$-reduction and the following notion of $\eta$-reduction:

\[
\frac{\lambda x.tx \triangleright_\eta \quad (x \notin \text{FV}(t))}{(x \notin \text{FV}(t))}
\]

Definition 3.51.

(1) We let $\triangleright_{\beta\eta}$ be the least compatible relation containing $\triangleright_\beta$ and $\triangleright_\eta$.

(2) We let $=_{\beta\eta}$ be the least congruence containing $\triangleright_{\beta\eta}$.

Example 3.52. Given $\lambda$-terms $t$ and $u$, let $t \circ u := \lambda x.t(ux)$. We have
\[
\begin{align*}
t \circ \text{id} & = \lambda x.t(\text{id} x) \triangleright_\beta \lambda x.tx \triangleright_\eta t \\
\text{id} \circ t & = \lambda x.\text{id}(t x) \triangleright_\beta \lambda x.tx \triangleright_\eta t
\end{align*}
\]

We shall now see that the relation $\equiv$ is precisely $=_{\beta\eta}$. See [SU06, Prop. 1.3.10] (also [Bar84, Prop. 3.3.2]). We first make the following simple observation.

Lemma 3.53. If $t \equiv u$ then $\lambda x.t \equiv \lambda x.u$. 

33
3. The Untyped Lambda-Calculus

Proof. Exercise! □

Proposition 3.54. Given λ-terms t, u, the following are equivalent:

(i) \( t \cong u \)

(ii) \( t =_{\beta\eta} u \)

Proof. Exercise! □

The reduction relation \( \triangleright_{\beta\eta} \) is confluent, see [Kri93, Thm. 1.30] or [Bar84, Thm. 3.3.9].

Proposition 3.55. The relation \( \approx_{\beta\eta} \) is confluent. In particular, the equational theory \( =_{\beta\eta} \) is consistent (via Prop. 3.21). A striking property of \( =_{\beta\eta} \) is that it is a maximal consistent equational theory on normalizable \( \lambda \)-terms. See [Bar84, Cor. 10.4.3] or [Kri93, §5].

Theorem 3.56 (Böhm). Let t, u be two \( \beta\eta \)-normal forms such that \( t \not=_{\beta\eta} u \). Let \( \cong_{(t,u)} \) be the least congruence containing \( =_{\beta\eta} \) and such that \( t \cong_{(t,u)} u \). Then \( \cong_{(t,u)} \) is inconsistent, i.e. \( v \cong_{(t,u)} w \) for all \( \lambda \)-terms \( v, w \).

Note that Thm. 3.56 still holds if \( t \) and \( u \) are only assumed to be \( \beta\eta \)-normalizable.

Remark 3.57. The assumption that \( t \) and \( u \) are \( \beta\eta \)-normalizable is essential for Thm. 3.56 since there are consistent extensions of \( =_{\beta\eta} \) on non-normalizable \( \lambda \)-terms. See [Bar84, Chap. 4].

Remark 3.58. The (restriction of the) relation \( =_{\beta\eta} \) on typed \( \lambda \)-terms (§4) is essential for denotational semantics.\(^4\)

3.7. Combinatory Logic

We briefly discuss a presentation of Combinatory Logic, a simple framework with no primitive notion of \( \lambda \)-abstraction, but in which \( \lambda \)-abstractions can be represented.

The terms of combinatory logic are given by

\[ t, u \in C \quad ::= \quad x \quad \mid \quad t \ u \quad \mid \quad s \quad \mid \quad k \]

where \( x \in X \) (§3.2.1). Note that the closed terms of combinatory logic are given by

\[ t, u \in C_0 \quad ::= \quad t \ u \quad \mid \quad s \quad \mid \quad k \]

We write \( t[u/x] \) for the substitution of \( x \) by \( u \) in \( t \). The conversion relation \( =_{sk} \) is the least binary relation on \( C \) which is closed under the following rules:

\[
\begin{align*}
\frac{}{t =_{sk} t} & \\
\frac{t =_{sk} u}{u =_{sk} t} & \\
\frac{t =_{sk} u}{t =_{sk} u} & \\
\frac{u =_{sk} v}{t =_{sk} v} & \\
\frac{t =_{sk} u \quad u =_{sk} u'}{t u =_{sk} t' u'} & \\
\frac{k \ t \ u}{t =_{sk} t} & \\
\frac{s \ t \ u \ v}{s =_{sk} t \ v \ (u \ v)}
\end{align*}
\]

We write \( =_{sk_0} \) for the least relation on \( C_0 \) closed under the above rules.

\(^4\)See e.g. [AC98, §4.2–4.6] (outside the scope of this course).
3. The Untyped Lambda-Calculus

**Lemma 3.59.** For each term \( t \), we have \((s \, k \, k \, t) =_{sk} t\). Moreover, \((s \, k \, k \, t) =_{skO} t\) if \( t \) is closed.

We now discuss a coding of lambda-abstractions using the combinators \( s \) and \( k \). Given a term \( t \in C \) and a variable \( x \), define the term \( \lambda x.t \in C \) by induction on \( t \):

\[
\begin{align*}
\lambda x.x & := s \, k \, k \\
\lambda x.t & := k \, t \quad \text{if } x \text{ does not occur in } t \\
\lambda x.(tu) & := s \, (\lambda x.t) \, (\lambda x.u)
\end{align*}
\]

Note that \( x \) does not occur in \( \lambda x.t \). Moreover, \( \lambda x.t \) is closed if \( t \) has no other variable than \( x \).

**Remark 3.60.** The above definition of \( \lambda x.t \) is consistent with [Bar84, Def. 7.1.5]. A possible variant of \( \lambda x.t \) is given by the following (see [Bar84, Def. 7.3.4]):

\[
\begin{align*}
\lambda x.x & := s \, k \, k \\
\lambda x.y & := k \, y \quad \text{if } y \neq x \\
\lambda x.t & := k \, t \quad \text{if } t \in \{s, k\} \\
\lambda x.(tu) & := s \, (\lambda x.t) \, (\lambda x.u)
\end{align*}
\]

**Lemma 3.61.** For all terms \( t \) and \( u \), we have \((\lambda x.t)u =_{sk} t[u/x]\). Moreover, \((\lambda x.t)u =_{skO} t[u/x]\) if \( t \) and \( u \) are closed.

**Proof.** Exercise!

3.7.1. Representation of Beta-Conversion

In view of Lem. 3.61, it makes sense to consider the following translation \( C(\_) \) of \( \lambda \)-terms (see [Bar84, Def. 7.3.1]):

\[
\begin{align*}
C(x) & := x \\
C(tu) & := C(t) \, C(u) \\
C(\lambda x.t) & := \lambda x.C(t)
\end{align*}
\]

Note that \( C(t) \) is closed if \( t \) is a closed \( \lambda \)-term.

We would have liked to have \( C(t) =_{sk} C(u) \) whenever \( t =_{\beta} u \), but this unfortunately does not hold, essentially because \( =_{sk} \) is too weak to be stable under the rule

\[
\frac{t =_{sk} u}{\lambda x.t =_{sk} \lambda x.u}
\]

**Example 3.62.** Consider the \( \lambda \)-term \( t := \lambda x.\text{id} \, x \). We obviously have \( t =_{\beta} \text{id} \), but we do not have \( C(t) =_{sk} C(\text{id}) \). First, note that

\[
C(\text{id}) = \lambda x.x = s \, k \, k
\]

so that

\[
C(t) = \lambda x.(s \, k \, k \, x) = s(k(s \, k \, k))(s \, k \, k)
\]
3. The Untyped Lambda-Calculus

\[ k =_{sk} \lambda x. \lambda y. kxy \quad k =_{sk} \lambda x. \lambda y. x \]

\[ s =_{sk} \lambda x. \lambda y. \lambda z. sxyz \quad s =_{sk} \lambda x. \lambda y. \lambda z. xy(yz) \]

\[ \lambda x. \lambda y. \lambda z. s(kx)(ky) =_{sk} \lambda x. \lambda y. k(xy) \]

\[ \lambda x. \lambda y. \lambda z. s(s(kk)x)y =_{sk} \lambda x. \lambda y. \lambda z. xz \]

\[ \lambda x. \lambda y. \lambda z. s(s(s(ks)x)y)z =_{sk} \lambda x. \lambda y. \lambda z. s(sxz)(syz) \]

Figure 3: Additional Conversion Rules Combinatory Logic.

However it can be shown that \( s(k(s k k))(s k k) \neq_{sk} s k k \). This follows from Prop. 3.21 (§3.4) and the confluence of the compatible closure \((C)\) of the relation \( \triangleright_{sk} \) given by

\( stuv \triangleright_{sk} t(v(u)) \) and \( ktu \triangleright_{sk} t \)

(see e.g. [Bar84, 7.2.4]).

The following is [Bar84, Thm. 7.3.10], where \( =_{sk} \) (resp. \( =_{sk0} \)) is the extension of \( =_{sk} \) (resp. of \( =_{sk0} \)) with the rules of Fig. 3 (which actually only consist of closed terms).

**Theorem 3.63.** Given \( \lambda \)-terms \( t \) and \( u \), we have \( t =_{\beta} u \) if and only if \( C(t) =_{sk} C(u) \). If \( t \) and \( u \) are closed, then \( t =_{\beta_0} u \) if and only if \( C(t) =_{sk0} C(u) \).

**Remark 3.64.** Actually [Bar84, Thm. 7.3.10], only gives the part of Thm. 3.63 on open \( \lambda \)-terms. Consider the case of \( t, u \in \Lambda_0 \) with \( t =_{\beta_0} u \). Then we obviously have \( t =_{\beta} u \) and thus \( C(t) =_{sk} C(u) \). Now, since \( =_{sk0} \) is closed under substitution, if the derivation of \( C(t) =_{sk} C(u) \) involves some variables, then they can be substituted by closed terms, and we indeed get \( C(t) =_{sk0} C(u) \).

Our motivation for Thm. 3.63 is the following consequence of Cor. 3.28 (§3.4.1):

**Corollary 3.65.** The following problems are undecidable:

- Given \( t, u \in C \), decide whether \( t =_{sk} u \).
- Given \( t, u \in C_0 \), decide whether \( t =_{sk0} u \).

We shall see in §6.2.4 (Thm. 6.35) that Cor. 3.65 gives a very simple proof of undecidability of (intuitionistic) first-order logic.
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

4.1. Introduction

This Section presents the Curry-Howard correspondence for intuitionistic propositional logic:

<table>
<thead>
<tr>
<th>Logic</th>
<th>Prog. Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formulae</td>
<td>Types</td>
</tr>
<tr>
<td>Proofs</td>
<td>Programs</td>
</tr>
</tbody>
</table>

We proceed in two steps. We present in §4.3 the Curry-Howard correspondence between natural deduction for intuitionistic minimal implicational logic (§2.4) and the simply-typed \(\lambda\)-calculus (STLC) (to be defined in §4.2). The simply-typed \(\lambda\)-calculus is a restriction on the formation of \(\lambda\)-terms (§3.2) based on a notion of simple types, which actually precisely amounts to:

<table>
<thead>
<tr>
<th>Intuitionistic Formulae</th>
<th>Simply-Typed Simple Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proofs</td>
<td>Typed (\lambda)-Terms</td>
</tr>
</tbody>
</table>

We then consider in §4.4 the case of natural deduction for full intuitionistic propositional logic (NJ\(_0\)). This amounts to extend the simply-typed \(\lambda\)-calculus with product and sum types.

Fundamental properties of intuitionistic logic (Thm. 2.9, §2.1) will be inferred from normalization properties of the simply-typed \(\lambda\)-calculus (in the sense of §3.4.3), which shall be discussed in §5.

On technical matters, besides [SU06, §3 & §4], we refer to [Gal95] and [GLT89, §3]. Again, beware that we should consistently follow the notations and technical definitions of none of these sources.

We refer to [SU06, §4.8] and [Gal95] for historical aspects. Let us just mention that an informal conceptual prequel of the Curry-Howard correspondence is the Brouwer-Heyting-Kolmogorov (BHK) interpretation of proofs of intuitionistic propositional logic. The BHK interpretation may be formulated as follows (where the term “proof” should be understood as some informal notion of “witness of evidence”):

- a “proof” of \(A_1 \land A_2\) is a pair of a “proof” of \(A_1\) and a “proof” of \(A_2\);
- a “proof” of \(A_1 \lor A_2\) is a (dependent) pair of an \(i \in \{1, 2\}\) and a “proof” of \(A_i\);
- a “proof” of \(A \Rightarrow B\) is a “function” taking a “proof” of \(A\) to a “proof” of \(B\);
- there is no “proof” of \(\bot\).

In particular, the BHK interpretation does not specify what should be understood as a “function” in the case of \(A \Rightarrow B\). We refer to [SU06, §2.1] and [TvD88a, Chap. 1, §3.1] for more on the BHK interpretation.
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

4.2. The Simply-Typed Lambda-Calculus

We introduce here a restriction on the formation of $\lambda$-terms based on a notion of typing (or typing discipline). There are a lot of notions of typing for the $\lambda$-calculus. Besides [SU06], a good synthetic but general account is [Bar92], while [Pie02] is a gentle but comprehensive reference from the point of view of programming languages.\(^5\)

We begin with the simplest notion, namely the (Curry-style) simply-typed $\lambda$-calculus, which is at the basis (at least conceptually) of most of typing disciplines for $\lambda$-terms.

We shall show in §5 that the simply-typed $\lambda$-calculus is strongly normalizing (recall from Ex. 3.34 (§3.4.3) that not every $\lambda$-term is normalizing). Under the Curry-Howard correspondence, the types of the simply-typed $\lambda$-calculus will be identified with the formulae of (intuitionistic) minimal implicational logic (§2.4); typed $\lambda$-terms will then correspond to (natural deduction) intuitionistic proofs (see §4.3).

Good technical references are [SU06, §4] and [Bar92, §3] (yet again with different notations and technical choices).

4.2.1. Syntax

We consider the following grammar of simple (function) types:

$$U, T, V ::= \kappa \mid U \rightarrow T$$

where $\kappa$ ranges over some (unspecified) set of base types.

Notation 4.1. Similarly as for formulae (Notation 2.2, §2), we assume that the arrow type constructor $\rightarrow$ associates to the right, so that $V \rightarrow U \rightarrow T$ stands for $V \rightarrow (U \rightarrow T)$ (which is different from $(V \rightarrow U) \rightarrow T$).

Simple types will be used to restrict the formation of $\lambda$-terms (§3.2). Recall that the latter are given by the grammar:

$$t, u \in \Lambda ::= x \mid \lambda x.t \mid tu$$

where $x$ ranges over the set $X$ of variables.

A typing context (or typing environment) is a list $E$ of the form $x_1 : U_1, \ldots, x_n : U_n$ where $x_1, \ldots, x_n \in X$ and such that $x_i \neq x_j$ whenever $i \neq j$. When $E = x_1 : U_1, \ldots, x_n : U_n$, we sometimes write $\text{dom}(E)$ for the set $\{x_1, \ldots, x_n\}$. The notation $E, x : U$ always assume $x \notin \text{dom}(E)$.

A typing judgment is a triplet of the form

$$E \vdash t : T$$

Figure 4 lists the typing rules of the simply-typed $\lambda$-calculus. We say that:

- $t$ has type $T$ in the context $E$ when the judgment $E \vdash t : T$ is derivable with these rules;

\(^5\)An other interesting reference (but mostly outside the scope of this course) is [AC98].
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

\[(\text{VAR}) \quad \Gamma \vdash x : T \quad ((x : T) \in \Gamma)\]

\[(\to-\text{I}) \quad \Gamma, x : U \vdash t : T \quad \quad \Gamma \vdash \lambda x.t : U \to T \quad \quad \Gamma \vdash u : U \quad \frac{}{\Gamma \vdash tu : T}\]

Figure 4: Typing Rules of the Simply-Typed \(\lambda\)-Calculus.

- \(t\) is typable in the context \(\Gamma\) when there exists a type \(T\) such that \(\Gamma \vdash t : T\) is derivable;
- \(t\) is typable when there exist some context \(\Gamma\) and some type \(T\) such that \(\Gamma \vdash t : T\) is derivable;
- \(T\) is inhabited if there is some \(\lambda\)-term \(t\) such that \(\vdash t : T\).

The following refer to \(\lambda\)-terms defined in Ex. 3.1 (§3.2.2).

Example 4.2.

1. For each type \(T\) we have \(\vdash \text{id} : T \to T\) with derivation tree:

\[\frac{x : T \vdash T}{\vdash \lambda x. x : T \to T}\]

2. For each types \(U, T, V\), with have \(\vdash \text{pair} : U \to T \to (U \to T \to V) \to V\) with the following derivation tree (where \(E\) is the context \(x : U, y : T, k : U \to T \to V\)):

\[\frac{\Gamma \vdash k : U \to T \to V \quad \Gamma \vdash x : T \quad \Gamma \vdash y : T}{\vdash k x y : T \to \Gamma \vdash \lambda k. k x y : (U \to T \to V) \to V \quad \Gamma \vdash \lambda x. \lambda y. \lambda k. k x y : U \to T \to (U \to T \to V) \to V \quad \vdash \lambda x. \lambda y. \lambda k. k x y : U \to T \to (U \to T \to V) \to V}]

Exercise 4.3. Derive the following typing judgments:

1. \(\vdash T : U \to T \to U\)
2. \(\vdash F : U \to T \to T\)
3. \(\vdash S : \text{nat}[T] \to \text{nat}[T]\), where \(\text{nat}[T] = T \to (T \to T) \to T\).

Exercise 4.4. Show that for each \(n \in \mathbb{N}\), we have \(\vdash n : \text{nat}[T]\).
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

4.2.2. Main Properties

We gather here some important basic properties of the simply-typed \( \lambda \)-calculus. See [SU06, §3] for more.\(^6\) In the following, the notation \( \triangleright_{\beta} \) refers to the full relation of \( \beta \)-reduction (Def. 3.12, §3.3.3).

We begin with simple basic properties, which are proved by induction on derivations.

**Fact 4.5** (Inversion).

1. If \( \mathcal{E} \vdash x : T \), then \( (x : T) \in \mathcal{E} \).
2. If \( \mathcal{E} \vdash \lambda x.t : T \), then \( T \) is of the form \( V \to U \) and \( \mathcal{E}, x : V \vdash t : U \).
3. If \( \mathcal{E} \vdash tu : T \) then there is some \( U \) such that \( \mathcal{E} \vdash t : U \to T \) and \( \mathcal{E} \vdash u : U \).

**Exercise 4.6.** Show that \( \delta \) (and thus \( \Omega \)) is not typable.

**Lemma 4.7** (Structural Properties).

(Weakening) If \( \mathcal{E} \vdash t : T \) and \( x \notin \text{dom}(\mathcal{E}) \) then \( \mathcal{E}, x : U \vdash t : T \).

(Contraction) If \( \mathcal{E}, x : U, y : U \vdash t : T \) then \( \mathcal{E}, x : U \vdash t[x/y] : T \).

(Exchange) If \( \mathcal{E}, x : U, \mathcal{E}', y : V, \mathcal{E}'' \vdash t : T \), then \( \mathcal{E}, y : V, \mathcal{E}', x : U, \mathcal{E}'' \vdash t : T \).

**Example 4.8.** Assuming \( \mathcal{E} \vdash t : U \to T \) and \( \mathcal{E} \vdash u : V \to U \), we have \( \mathcal{E} \vdash t \circ u : V \to T \) (where \( t \circ u := \lambda x.t(ux) \)), with derivation tree:

\[
\begin{array}{c}
E \vdash \lambda x.t(ux) : V \to T \\
E, x : V \vdash t(ux) : T \\
E, x : V \vdash u : V \\
E, x : V \vdash t : U \\
E \vdash t \circ u : V \to T \\
\end{array}
\]

The following two properties are required for essentially all type systems.\(^7\)

**Lemma 4.9** (Substitution). If \( \mathcal{E}, x : U \vdash t : T \) and \( \mathcal{E} \vdash u : U \) then \( \mathcal{E} \vdash t[u/x] : T \).

**Proposition 4.10** (Subject Reduction). If \( \mathcal{E} \vdash t : T \) and \( t \triangleright_{\beta} u \) then \( \mathcal{E} \vdash u : T \).

**Remark 4.11.** In particular, for a typing context \( \mathcal{E} \) and a type \( T \), the relation \( \triangleright_{\beta} \) is confluent on the set

\[ |\mathcal{E} \vdash T| := \{ t \mid \mathcal{E} \vdash t : T \} \]

The following fundamental property of the simply-typed \( \lambda \)-calculus is admitted until §5 (Thm. 5.32, §5.5). Recall from Ex. 3.34 (§3.4.3) that the (non typable) \( \lambda \)-term \( \Omega \) is not normalizing for \( \beta \)-reduction.

\(^6\)See also [AC98, §4.5] (beyond the scope of this course).

\(^7\)Type systems for variants of STLC with other notions of reduction would require different formulations. A (non basic but) relevant example is [Lev03, Prop. 10, §2].
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

<table>
<thead>
<tr>
<th>Simple Types</th>
<th>$\equiv$</th>
<th>$\Rightarrow$-Formulae</th>
</tr>
</thead>
<tbody>
<tr>
<td>(base types)</td>
<td>$\kappa$</td>
<td>$\equiv$</td>
</tr>
<tr>
<td>(function types)</td>
<td>$(-) \to (-)$</td>
<td>$\equiv$ $(-) \Rightarrow (-)$</td>
</tr>
</tbody>
</table>

Table 1: The Curry-Howard Correspondence: Simple Types and $\Rightarrow$-Formulae.

**Theorem 4.12** (Strong Normalization). If $E \vdash t : T$ then $t$ is strongly $\beta$-normalizing (in the sense of Def. 3.33, §3.4.3).

Theorem 4.12 is a particular case of Thm. 4.31 (§4.4.4).

**Remark 4.13** (Decidability of Typing). The following are decidable problems:

(1) Given a type $T$, a context $E$ and a $\lambda$-term $t$, decide whether $E \vdash t : T$.

(2) Given a $\lambda$-term $t$, decide whether $t$ is typable.

Decidability of type inhabitation is discussed in Rem. 4.20 (§4.3) below. We refer to [SU06, §3.2] for details.

4.3. Curry-Howard Correspondence for Intuitionistic Minimal Implicational Logic

Recall that the formulae of minimal implicational logic (§2.4) are given by

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

where $p$ is an atomic proposition.

On the other hand, the simple (function) types of §4.2.1 are given by

$$U, T ::= \kappa \mid U \to T$$

where $\kappa$ is a base type.

The Curry-Howard correspondence for intuitionistic minimal implicational logic stems from the identification of simple (arrow) types with the formulae of minimal implicational logic (see Tab. 1). Under this identification, we may consider that simple types are formulae of minimal implicational logic.

**Notation 4.14** (Types as Formulae). For the remaining of this §4.3 we assume that types are given by the grammar of formulae:

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

41
This leads to a strong analogy between typing rules on the one hand and deduction rules on the other hand. More precisely, erasing terms (and variables) from the typing rules of Fig. 4 (§4.2.1) exactly gives the deduction rules of §2.4:

\[
\begin{align*}
\frac{x_1 : A_1, \ldots, x_n : A_n \vdash x_i : A_i}{\vdash A_1, \ldots, A_n \vdash A_i} & \quad \text{(Ax)} \\
\frac{x_1 : A_1, \ldots, x_n : A_n, x : A \vdash t : B}{\vdash A_1, \ldots, A_n, A \vdash B} & \quad \text{($\Rightarrow$-I)} \\
\frac{x_1 : A_1, \ldots, x_n : A_n \vdash t : A \Rightarrow B}{\vdash A_1, \ldots, A_n \vdash A \Rightarrow B} & \quad \text{($\Rightarrow$-E)} \\
\frac{x_1 : A_1, \ldots, x_n : A_n \vdash u : A}{\vdash A_1, \ldots, A_n \vdash B} & \quad \text{($\Rightarrow$-E)}
\end{align*}
\]

It follows that typed $\lambda$-terms can be identified with proofs:

<table>
<thead>
<tr>
<th>Intuitionistic</th>
<th>Simply-Typed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min. $\Rightarrow$-Logic</td>
<td>$\lambda$-Calculus</td>
</tr>
<tr>
<td>Formulae</td>
<td>$\equiv$</td>
</tr>
<tr>
<td>Proofs</td>
<td>$\equiv$</td>
</tr>
</tbody>
</table>

In particular, we have the following obvious result, stated as a Theorem for emphasis.

**Theorem 4.15** (Curry-Howard Correspondence). The sequent $A_1, \ldots, A_n \vdash A$ is derivable in intuitionistic minimal implicational logic if and only if there is a $\lambda$-term $t$ such that $x_1 : A_1, \ldots, x_n : A_n \vdash t : A$.

**Remark 4.16.** As a direct consequence of Thm. 4.15 (together with Prop. 2.34, §2.4), note that if $p, q$ are distinct atomic propositions, then there is no $\lambda$-term $t$ such that $\vdash t : ((p \Rightarrow q) \Rightarrow p) \Rightarrow p$.

On the other hand, Thm. 4.15 of course gives $\lambda$-terms for all intuitionistic tautologies of minimal implicational logic.

We now consider examples inspired from §2.2. Since we have no proper $\bot$ yet (and thus no proper negation), we replace $\bot$ by a chosen atomic proposition $R$ and write $\neg_R A$ for $A \Rightarrow R$. Note that the rule (ExFalso) is unavoidable: we are indeed in minimal logic (see Rem. 2.16).

**Example 4.17.** We have $\lambda a.\lambda k.ka : A \Rightarrow \neg_R \neg_R A$ with the derivation

\[
\frac{a : A, k : \neg_R A \vdash k : A \Rightarrow R}{\vdash a : A, k : \neg_R A \vdash \lambda k.ka : R} \quad \frac{x : A, k : \neg_R A \vdash a : A}{\vdash a : A \Rightarrow \lambda k.ka : \neg_R \neg_R A}
\]

**Exercise 4.18.** In each case below, give a $\lambda$-term $t$ of the prescribed type:

(1) $\vdash t : \neg_R \neg_R \neg_R A \Rightarrow \neg_R A$

(2) $\vdash t : (A \Rightarrow B) \Rightarrow (\neg_R \neg_R A \Rightarrow \neg_R \neg_R B)$
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

$$\vdash t : (\neg_r \neg_r A \Rightarrow \neg_r \neg_r B) \Rightarrow \neg_r \neg_r A$$

In contrast with Rem. 4.16, it is not too difficult to find λ-terms for the Kolmogorov translation of Peirce’s law (Rem. 2.43, §2.5).

**Exercise 4.19.** Give a λ-term t such that $\vdash t : \neg_r \neg_r (\neg_r \neg_r A \Rightarrow \neg_r \neg_r B) \Rightarrow \neg_r \neg_r A$.

**Remark 4.20** (Decidability of Type Inhabitation). Continuing Rem. 4.13 (§4.2), it follows from Thm. 4.15 and the decidability of provability in intuitionistic minimal implicational logic (Rem. 2.36, §2.4) that the following type inhabitation problem is decidable:

- Given a type T, decide whether T is inhabited.

We refer to [SU06, §4.2] for more.

4.3.1. Beta-Reduction and Curry-Howard

Theorem 4.15 extends to a correspondence between β-reduction and a notion of computation for natural deduction called proof normalization. The idea is that a step of β-reduction

\[
\frac{
\text{\Pi}_1 \vdash \lambda x.t : A \Rightarrow B \\
\text{\Pi}_2 \vdash u : A \\
\text{\Pi}_1[\Pi_2/x] \vdash t[u/x] : B
}{\text{\E \vdash \lambda x.t : A \Rightarrow B}}
\]

(where the derivation $\Pi_1[\Pi_2/x]$ is obtained by the Substitution Lemma 4.9, §4.2.2) corresponds to the reduction of redexes ($\Rightarrow$-I)/(⇒-E) in natural deduction:

\[
\frac{
\Delta, A \vdash B \\
\Delta \vdash A \Rightarrow B \\
\Delta \vdash A
}{\Delta \vdash B}
\]

Here, the proof

\[
\frac{
\Pi_1[\Pi_2/A] \\
\Delta \vdash B
}{\Delta \vdash A}
\]

stands for the proof $\Pi_1$ in which each (Ax) rule

\[
\frac{
\Delta' \vdash A
}{\Delta' \vdash A}
\]

(where $\Delta$ is necessarily a prefix of $\Delta'$) is replaced by a derivation of $\Delta' \vdash A$ obtained from $\Pi_2$ by weakenings (Lem. 2.6, §2.1).

We shall not pursue this direction too far. We refer to [SU06, §4.4], [vD04, §6] and [TS00, §6] for normalization of natural deduction proofs.
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

4.4. Full Intuitionistic Propositional Logic

We now turn to the Curry-Howard correspondence for the full system NJ₀ of §2.1. This requires an extension of the (simply-typed) λ-calculus that we introduce step by step. We mainly refer to [SU06, §4.5] (see also [Gal95, §3]). See [Pie02, §11] for a programming language perspective on the additional constructs introduced in §4.4.1–§4.4.3 below.

Notation 4.21. We step back from Notation 4.14 (§4.3) and consider for the moment types and formulae as different entities.

4.4.1. Intuitionistic Conjunctions and Products

The natural deduction rules for conjunction (−) ∧ (−), namely

\[
\frac{\Delta \vdash A \quad \Delta \vdash B}{\Delta \vdash A \land B} \quad (\land\text{-}I) \quad \frac{\Delta \vdash A \land B}{\Delta \vdash A} \quad (\land\text{-}E_1) \quad \frac{\Delta \vdash A \land B}{\Delta \vdash B} \quad (\land\text{-}E_2)
\]

suggest to extend the simply-typed λ-calculus with product types (−) × (−) (and the corresponding term formers), as in the following additional typing rules:

\[
\frac{E \vdash t : T \quad E \vdash u : U}{E \vdash \langle t, u \rangle : T \times U} \quad (\times\text{-}I) \quad \frac{E \vdash \langle t, u \rangle : T \times U \quad \Pi_1 t : T}{E \vdash t : T} \quad (\times\text{-}1\text{-}E) \quad \frac{E \vdash \langle t, u \rangle : T \times U \quad \Pi_2 t : U}{E \vdash u : U} \quad (\times\text{-}2\text{-}E)
\]

The term former ⟨−, −⟩ is usually called pairing, while π₁(−), π₂(−) are projections. Moreover (reversing the approach of §4.3.1), the reduction of (∧-I)/(∧-E)-redexes in natural deduction, namely

\[
\frac{\Pi_1 \vdash A_1 \quad \Pi_2 \vdash A_2}{\Pi_1 \vdash A_1 \land A_2} \quad \Delta \vdash A_i \quad \triangleright \quad \frac{\Pi_1 \vdash A_i}{\Delta \vdash A_i}
\]

suggests the following extension of β-reduction to cope with products and pairs:

\[
\pi_1(t_1, t_2) \triangleright_\beta t_1 \\
\pi_2(t_1, t_2) \triangleright_\beta t_2
\]

Finally, the 0-ary form ⊤ of (−) ∧ (−), with its (unique) natural deduction rule

\[
\frac{\top-\text{I}}{\Delta \vdash \top}
\]

suggests a 0-ary form of (−) × (−), i.e. a unit type unit with term former ⟨⟩ typed as

\[
\frac{\text{unit-I}}{E \vdash \langle \rangle : \text{unit}}
\]
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

4.4.2. Intuitionistic Disjunctions and Sums

Consider now the natural deduction rules for (intuitionistic) disjunction (-) ∨ (-):

\[
\begin{align*}
\text{ (∨-I) } & \quad \Delta \vdash A_i \\
\text{ (∨-E) } & \quad \Delta \vdash A_1 \lor A_2 
\end{align*}
\]

These rules correspond closely to the following rules for sum types (-) + (-):

\[
\begin{align*}
\text{ (+-I) } & \quad E \vdash t : T_i \\
\text{ (+-E) } & \quad \frac{E \vdash \text{case } t \{ \text{in}_1 \ x_1 \mapsto u_1 | \text{in}_2 \ x_2 \mapsto u_2 \} : U}{E \vdash t : T_1 + T_2}
\end{align*}
\]

The term formers \(\text{in}_1(-), \text{in}_2(-)\) are called coprojections. \(^8\) The case construction (which comes under various names and notations in different settings) is a close relative of the usual pattern matching constructs of (functional) programming languages, while sum types are a form of variant type (see [Pie02, §11.8 & §11.9]).

The reduction of (∨-I)/(∨-E)-redexes in natural deduction:

\[
\begin{align*}
\Pi \vdash A_i & \quad \Pi_1 \vdash C \\
\Delta \vdash A_1 \lor A_2 & \quad \Delta, A_1 \vdash C \\
\Delta \vdash C & \quad \Delta, A_2 \vdash C
\end{align*}
\]

(\(\Pi_i[\Pi/A_i]\) is obtained similarly as in §4.3.1) closely corresponds to the usual reduction rules for pattern matching:

\[
\begin{align*}
\text{ case } (\text{in}_1 \ t) \{ \text{in}_1 \ x_1 \mapsto u_1 | \text{in}_2 \ x_2 \mapsto u_2 \} & \quad \triangleright \quad u_1[t/x_1] \\
\text{ case } (\text{in}_2 \ t) \{ \text{in}_1 \ x_1 \mapsto u_1 | \text{in}_2 \ x_2 \mapsto u_2 \} & \quad \triangleright \quad u_2[t/x_2]
\end{align*}
\]

(where that \(t\) is of type \(U_i\) when \(\text{in}_i \ t\) is of type \(U_1 + U_2\)).

Consider now \(\bot\), the 0-ary case of (-) ∨ (-) with (unique) natural deduction rule \(\text{(-E)}\):

\[\Delta \vdash \bot\]

This suggests a 0-ary version of (-) + (-), which is provided by the empty type \(\text{void}\) with elimination form \(\text{(void-E)}\):

\[\frac{E \vdash \text{case } \bot \{ \} : T}{E \vdash \text{void} : T}\]

Note that the (void-E)-rule produces a term of any type \(T\)!

Remark 4.22. Natural deduction is often equipped with stronger reduction rules for (intuitionistic) disjunction than the above, see e.g. [Gal95] and [TS00, §6].

\(^8\) An other usual name is “injection” (but it may wrongly suggest an injectivity property).
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

Basic Rules:

\[(\lambda x.t)u \xrightarrow{0} t[u/x]\]
\[\pi_1(t,u) \xrightarrow{0} t \quad \text{case } (in_1) \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto u_2 \} \} \xrightarrow{0} \{ u_1[t/x] \}
\]
\[\pi_2(t,u) \xrightarrow{0} u \quad \text{case } (in_2) \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto u_2 \} \} \xrightarrow{0} \{ u_2[t/x] \}
\]

Congruence Rules: \(\xrightarrow{\beta}\) is the least relation containing \(\xrightarrow{0}\) and closed under the rules

\[
\begin{align*}
(t \xrightarrow{\beta} t') &\Rightarrow (tu \xrightarrow{\beta} t'u) & (t \xrightarrow{\beta} t') &\Rightarrow (\lambda x.t \xrightarrow{\beta} \lambda x.t') \\
\pi_1 t \xrightarrow{\beta} \pi_1 t' &\Rightarrow \pi_2 t \xrightarrow{\beta} \pi_2 t' & \langle t,u \rangle \xrightarrow{\beta} \langle t',u \rangle &\Rightarrow \langle t,u \rangle \xrightarrow{\beta} \langle t,u' \rangle \\
\text{case } t \{ \} \xrightarrow{\beta} \text{case } t' \{ \} &\Rightarrow \text{case } (in_1) \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto u_2 \} \} \xrightarrow{\beta} \text{case } t' \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto v \} \} \\
\text{case } t \{ \{ \text{in}_1 x \mapsto u \mid \text{in}_2 x \mapsto v \} \} \xrightarrow{\beta} \text{case } t \{ \{ \text{in}_1 x \mapsto u' \mid \text{in}_2 x \mapsto v \} \} &\Rightarrow \text{case } t \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto v \} \} \xrightarrow{\beta} \text{case } t \{ \{ \text{in}_1 x \mapsto u' \mid \text{in}_2 x \mapsto v' \} \}
\end{align*}
\]

Figure 5: The Relation of Full (Strong) \(\beta\)-Reduction.

4.4.3. A Simply-Typed Lambda-Calculus with Sums and Products

To summarize, we end up with a type system for extended \(\lambda\)-terms given by the grammar:

\[
t,u ::= x \mid \lambda x.t \mid tu \mid \langle t,u \rangle \mid \pi_1 t \mid \pi_2 t \\
\mid \{ \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto u_2 \} \} \mid \text{case } t \{ \}
\]

where \(x \in X\) (as in §3).

Warning 4.23. The case construct actually incorporates binders: the variables \(x_1, x_2\) are bound in case \(t \{ \{ \text{in}_1 x_1 \mapsto u_1 \mid \text{in}_2 x_2 \mapsto u_2 \} \}. We thus assume the corresponding extension of \(\alpha\)-conversion (§3.2.3 and §3.2.4).

The notions of free-variable (Def. 3.3, §3.2.3) and of capture-avoiding substitution (Def. 3.8, §3.3) are adapted accordingly.

As for reduction, we consider the analogue of Def. 3.12 (§3.3.3) for the extended \(\lambda\)-terms defined above. More precisely, we first define a basic reduction relation \(\xrightarrow{0}\) with
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

\[
\begin{align*}
\text{(VAR)} & \quad \frac{}{\emptyset \vdash x : T} \quad (\text{unit-I}) & \quad \frac{}{\emptyset \vdash \langle \rangle : \text{unit}} \quad (\text{void-E}) & \quad \frac{\emptyset \vdash t : \text{void}}{\emptyset \vdash \text{case}_1 t \{\} : T} \\
(\to-I) & \quad \frac{\emptyset, x : U \vdash t : T}{\emptyset \vdash \lambda x. t : U \to T} \quad (\to-E) & \quad \frac{\emptyset \vdash t : U \to T \quad \emptyset \vdash u : U}{\emptyset \vdash tu : T} \\
(\times-I) & \quad \frac{\emptyset \vdash t_1 : T_1 \quad \emptyset \vdash t_2 : T_2}{\emptyset \vdash \langle t_1, t_2 \rangle : T_1 \times T_2} \quad (\times-E) & \quad \frac{\emptyset \vdash t : T_1 \times T_2}{\emptyset \vdash \pi_1 t : T_1} \quad \frac{\emptyset \vdash t : T_1 \times T_2}{\emptyset \vdash \pi_2 t : T_2} \\
(+I) & \quad \frac{\emptyset \vdash t_1 : T_1 \quad \emptyset \vdash t_2 : T_2 + T_1}{\emptyset \vdash \text{in}_1 t : T_1 + T_2} \quad (+-E) & \quad \frac{\emptyset, x_1 : T_1 \vdash u_1 : U \quad \emptyset, x_2 : T_2 \vdash u_2 : U}{\emptyset \vdash \text{case}_1 t \{\text{in}_1 x_1 \mapsto u_1 \mid \text{in}_2 x_2 \mapsto u_2\} : U}
\end{align*}
\]

Figure 6: Typing Rules with Sums and Products.

the basic rules of Fig. 5. We then let the full \textbf{(strong)} reduction relation \(\triangleright_\beta\) be the closure of \(\triangleright_0\) under the congruence rules of Fig. 5.

\textbf{Warning 4.24.} What we call \(\beta\)-reduction here is often called differently in the literature, because the reduction rules for products, sums etc. are often given specific names.

We consider \textbf{types} given by the grammar

\[
T, U ::= \kappa \mid U \to T \mid T \times U \mid T + U \mid \text{unit} \mid \text{void}
\]

where \(\kappa\) ranges over some (unspecified) set of base types. The \textbf{typing relation} \(\emptyset \vdash \cdot : \cdot\) is defined by the rules of Fig. 6.

\textbf{Exercise 4.25} (Booleans). Let \(\text{bool} := \text{unit} + \text{unit}\) and

\[
\begin{align*}
\text{true} & \ ::= \ \text{in}_1 \{\} : \text{bool} \\
\text{false} & \ ::= \ \text{in}_2 \{\} : \text{bool}
\end{align*}
\]

Define \(\lambda\)-terms \(\text{neg} : \text{bool} \to \text{bool}\) and \(\text{and} : \text{bool} \times \text{bool} \to \text{bool}\) implementing resp. Boolean negation and conjunction.

In particular, all Boolean functions are definable by \(\lambda\)-terms. This extends to any finite “base type”.

\textbf{Exercise 4.26} (Finite Base Types). We define the type \(\sum_{i=1}^n T_i\) by induction on \(n \in \mathbb{N}\) as

\[
\begin{align*}
\sum_{i=1}^0 T_i & \ ::= \ \text{void} \\
\sum_{i=1}^{n+1} T_i & \ ::= \ T_1 + \sum_{i=1}^n T_{i+1}
\end{align*}
\]

47
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

Given a finite set \( A = \{a_1, \ldots, a_n\} \), the type \( A \) is \( \sum_{i=1}^{n} \text{unit} \). For each \( k = 1, \ldots, n \), let
\[
a_k := \text{in}_2 \cdots \text{in}_2 \text{in}_1 \langle \rangle : A
\]
k \(-1\) times

Assume \( A = \{a_1, \ldots, a_n\} \) and \( B = \{b_1, \ldots, b_m\} \). Show that for each function \( f : A \to B \) there is a \( \lambda \)-term \( f : A \to B \) such that
\[
f(a_k) \xrightarrow{\beta} b_\ell \text{ if and only if } f(a_k) = b_\ell
\]

4.4.4. Main Properties

We now discuss the extension of §4.2.2 to product and sum types.

The following are proved exactly as their counterparts in §4.2.2.

Fact 4.27 (Inversion).

1. If \( E \vdash x : T \), then \( (x : T) \in E \).
2. If \( E \vdash \lambda x.t : T \), then \( T \) is of the form \( V \to U \) and \( E, x : V \vdash t : U \).
3. If \( E \vdash tu : T \) then there is some \( U \) such that \( E \vdash t : U \to T \) and \( E \vdash u : U \).
4. If \( E \vdash (t_1, t_2) : T \) then \( T \) is of the form \( U_1 \times U_2 \) and \( E \vdash t_i : U_i \) for each \( i = 1, 2 \).
5. If \( E \vdash \pi_i t : T_i \) then there is some \( T_{3-i} \) such that \( E \vdash t : T_1 \times T_2 \).
6. If \( E \vdash \langle \rangle : T \) then \( T = \text{unit} \).
7. If \( E \vdash \text{in}_i t : T \) then \( T \) is of the form \( U_1 + U_2 \) and \( E \vdash t : U_1 \).
8. If \( E \vdash \text{case} \ t \{ \text{in}_1 x_1 \mapsto u_1 | \text{in}_2 x_2 \mapsto u_2 \} : T \), then there are some \( U_1, U_2 \) such that
   \( E \vdash t : U_1 + U_2 \) and \( E, x_i : U_i \vdash u_i : T \) for \( i = 1, 2 \).
9. If \( E \vdash \text{case}_\bot t \{ \} : T \) then \( E \vdash t : \text{void} \).

Lemma 4.28 (Structural Properties).

(Weakening) If \( E \vdash t : T \) and \( x \notin \text{dom}(E) \) then \( E, x : U \vdash t : T \).

(Contraction) If \( E, x : U, y : V \vdash t : T \) then \( E, x : U \vdash t[x/y] : T \).

(Exchange) If \( E, x : U, E' : V, E'' \vdash t : T \), then \( E, y : V, E', x : U, E'' \vdash t : T \).

Lemma 4.29 (Substitution). If \( E, x : U \vdash t : T \) and \( E \vdash u : U \) then \( E \vdash t[u/x] : T \).

Proposition 4.30 (Subject Reduction). If \( E \vdash t : T \) and \( t \xrightarrow{\beta} u \) then \( E \vdash u : T \).

We now turn to normalization. Theorem 4.12 (§4.2.2) extends to sums and products.

Theorem 4.31 (Strong Normalization). If \( E \vdash t : T \) then \( t \) is strongly \( \beta \)-normalizing (in the sense of Def. 3.33, §3.4.3).
Theorem 4.31 is admitted until §5 (Thm. 5.32, §5.5). Let us now discuss some of its corollaries.

First, concerning confluence, in contrast with the pure λ-calculus we shall not be concerned with the case of the untyped extended λ-calculus. We shall thus content ourselves with confluence on typed terms, which can be obtained using Newman’s Lemma 3.35 (§3.4.3) from Theorem 4.31 and local confluence (see [SU06, §4.5]). In the following, the notation |E ⊢ T| refers to the obvious adaptation of Rem. 4.11 (§4.2.2).

**Theorem 4.32.** For each typing context E and each type T, the relation ⊢ β is confluent on |E ⊢ T|.

Finally, we can state and prove the (relevant) analogue of Thm. 2.9 (§2.1). This relies on the following crucial fact on the shape of (typed) normal forms.

**Lemma 4.33 (Closed Typed Normal Forms).** If t is a closed typable λ-term in β-normal form, then t is of one of the following forms:

\[ \lambda x. u \quad \langle \rangle \quad \langle u, v \rangle \quad \text{in}_1 u \quad \text{in}_2 u \]

**Proof.** Exercise! □

Combining Lem. 4.33 with Strong Normalization (Thm. 4.31) and Subject Reduction (Prop. 4.30) readily gives the following.

**Corollary 4.34.** In the simply-typed λ-calculus with sums and products,

1. there is no λ-term t such that ⊢ t : void;
2. if ⊢ t : T_1 + T_2 then there are some i ∈ \{1, 2\} and some λ-term u_i such that t ⊢ β^* \text{in}_i u_i and ⊢ u_i : T_i.

Corollary 4.34 is proven without relying on Strong Normalization (Thm. 4.31) in §5.3 (Cor. 5.11).

4.4.5. Curry-Howard Correspondence

We now proceed to the Curry-Howard correspondence for the full intuitionistic propositional logic NJ_0.

We begin with the identification of types with formulae. First, recall their respective grammars:

\[
\begin{align*}
T, U & ::= \kappa \mid U \rightarrow T \mid T \times U \mid T + U \mid \text{unit} \mid \text{void} \\
A, B & ::= p \mid B \Rightarrow A \mid A \land B \mid A \lor B \mid \top \mid \bot
\end{align*}
\]

Extending §4.3, we shall further identify:

- conjunctions (−) ∧ (−) with product types (−) × (−) (and \top with unit);
- disjunctions (−) ∨ (−) with the sum types (−) + (−) (and \bot with void).
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

<table>
<thead>
<tr>
<th>Types</th>
<th>Formulae of Intuitionistic Prop. Logic</th>
</tr>
</thead>
<tbody>
<tr>
<td>(base types) κ</td>
<td>p (atomic propositions)</td>
</tr>
<tr>
<td>(functions) (−) → (−)</td>
<td>(−) ⇒ (−) (implications)</td>
</tr>
<tr>
<td>(products) (−) × (−)</td>
<td>(−) ∧ (−) (conjunctions)</td>
</tr>
<tr>
<td>(unit) unit</td>
<td>⊤ (truth)</td>
</tr>
<tr>
<td>(sums) (−) + (−)</td>
<td>(−) ∨ (−) (int. disjunctions)</td>
</tr>
<tr>
<td>(void) void</td>
<td>⊥ (falsity)</td>
</tr>
</tbody>
</table>

Table 2: The Curry-Howard Correspondence: Types and Formulae.

The resulting correspondence between types and formulae is summarized in Table 2. We may thus consider that types are formulae of propositional logic.

Notation 4.35 (Types as Formulae). Extending Notation 4.14 (§4.3), for the remaining of this §4.4.5 we assume that types given by the grammar of formulae:

\[ A, B ::= p \mid A \Rightarrow B \mid A \wedge B \mid A \vee B \mid \top \mid \bot \]

As depicted in Fig. 7, erasing λ-terms from typing rules exactly gives the derivation rules of NJ0. It follows that typed λ-terms can be identified with proofs:

<table>
<thead>
<tr>
<th>Intuitionistic Logic (NJ0)</th>
<th>Simply-Typed λ-Calculus (with +, ×)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formulae</td>
<td>Types</td>
</tr>
<tr>
<td>Proofs</td>
<td>Typed λ-Terms</td>
</tr>
</tbody>
</table>

Remark 4.36 (Proof-Terms). Under the Curry-Howard correspondence, typed λ-terms are often called proof-terms.

In particular, we have the following obvious extension of Thm. 4.15 (§4.3).

Theorem 4.37 (Curry-Howard Correspondence). The sequent \( A_1, \ldots, A_n \vdash A \) is derivable in NJ0 if and only if there is a λ-term \( t \) such that \( x_1 : A_1, \ldots, x_n : A_n \vdash t : A \).

Example 4.38. We have \( t : (A \vee \neg A) \Rightarrow (\neg A \Rightarrow A) \Rightarrow A \) where

\[ t : (A \vee \neg A) \Rightarrow (\neg A \Rightarrow A) \Rightarrow A \]

\[ := \lambda e. \lambda c. \text{case } e \{ \]

\[ \quad \text{in}_1 x_1 \mapsto x_1 \]

\[ \quad \text{in}_2 x_2 \mapsto c x_2 \} \]

since \( e : A \vee \neg A, c : \neg A \Rightarrow A \vdash \text{case } e \{ \]

\[ \quad \text{in}_1 x_1 \mapsto x_1 \]

\[ \quad \text{in}_2 x_2 \mapsto c x_2 \} : A \]
Figure 7: The Curry-Howard Correspondence: Typing and Deduction Rules.
### 4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

Together with Cor. 4.34 (§4.4.4), Thm. 4.37 gives the remaining part of Thm. 2.9 (§2.1).

**Corollary 4.39.** In intuitionistic propositional logic ($\text{NJ}_0$),

1. $\vdash \bot$ is not derivable;
2. if $\vdash A \lor B$ then either $\vdash A$ or $\vdash B$.

Similarly as in §4.3, we consider some examples from §2.

**Exercise 4.40.** In each case below, give a $\lambda$-term $t$ of the prescribed type:

1. $\vdash t : ((\neg A \Rightarrow A) \Rightarrow \neg \neg A \Rightarrow \neg A$
2. $\vdash t : (A \lor \neg A) \Rightarrow \neg \neg A \Rightarrow A$
3. $\vdash t : \neg \neg (A \lor \neg A)$

**Exercise 4.41.** In each case below, give a $\lambda$-term $t$ of the prescribed type:

1. $\vdash t : (B \land (A_1 \lor A_2)) \Rightarrow (B \land A_1) \lor (B \land A_2)$
2. $\vdash t : (B \land A_1) \lor (B \land A_2) \Rightarrow B \land (A_1 \lor A_2)$

**Remark 4.42.** The proof terms of Ex. 4.41 enforce a form of distributive law. Their mere existence is already due to deep semantic reasons, related to the interaction of $\Rightarrow / \rightarrow$ with $\land / \times$ and $\lor / +$.

Let us say a few words on this, in a simple setting which actually forms the basis of algebraic semantics of intuitionistic propositional logic (see e.g. [SU06, §2.4]). The following is somewhat beyond the scope of this course.

Define the preorder $\leq$ on formulae as $A \leq B$ if $A \vdash B$ in $\text{NJ}_0$. The relation $\leq$ becomes a partial order on formulae quotiented by the equivalence relation

$$A \equiv B \iff A \leq B \text{ and } B \leq A$$

The poset of quotiented formulae is actually a **lattice**, i.e. it has all finite sups and infs (see [SU06, Def. 2.3.1]) given resp. by the action of $\lor$ (with unit $\bot$) and $\land$ (with unit $\top$) on quotiented formulae.

Now, Ex. 4.41 says that this lattice is **distributive** ([SU06, Def. 2.3.5]) in the sense that it satisfies the following law:

$$\forall (C \lor B) \land A = (C \land A) \lor (B \land A)$$

(we confuse formulae with their equivalence classes). But beware that not every lattice is distributive! A well-known counter example is the lattice $\text{M}_3$, which can be depicted

---

9The two laws mentioned in [SU06, Def. 2.3.5] are actually equivalent in any lattice.
4. Curry-Howard Correspondence for Intuitionistic Propositional Logic

as follows:

\[
\begin{array}{c}
\top \\
\downarrow \\
a \\
\downarrow \\
b \\
\downarrow \\
c \\
\downarrow \\
\bot
\end{array}
\]

The distributive law above may be read as the preservation of \((-) \lor (-)\) by \((-) \land A\), and actually follows from the following property of logical implication \((-)\):

\[B \land A \leq C \iff B \leq A \Rightarrow C\]

**Remark 4.43.** Alternative syntaxes consider case’s of the following form (e.g. [Gal95]):

\[
\frac{\mathcal{E} \vdash t : A_1 + A_2 \quad \mathcal{E}, x_1 : A_1 \vdash u_1 : B \quad \mathcal{E}, x_2 : A_2 \vdash u_2 : B}{\mathcal{E} \vdash \text{case } t \{ \text{in}_1 \mapsto \lambda x_1. u_1 \mid \text{in}_2 \mapsto \lambda x_2. u_2 \} : B}
\]

**Remark 4.44** (On the BHK Interpretation). The Curry-Howard correspondence can be seen as an instance of the BHK interpretation (see §4.1). More precisely, under the Curry-Howard correspondence, Thm. 4.31 and Lem. 4.33 (§4.4.4) give the following (where by “proof” we understand “proof term in β-normal form”):

- a “proof” of \(A_1 \land A_2\) is a pair of a “proof” of \(A_1\) and a “proof” of \(A_2\);
- a “proof” of \(A_1 \lor A_2\) contains an \(i \in \{1, 2\}\) and a “proof” of \(A_i\);
- a “proof” of \(A \Rightarrow B\) is a “function” taking a “proof” of \(A\) to a “proof” of \(B\);
- there is no “proof” of \(\bot\).

Above, the word “function” can be understood to refer to those computable functions \(f\) such that for some \(\lambda\)-term \(\vdash \lambda x. t : A \Rightarrow B\), \(f\) takes a “proof” \(\vdash u : A\) to the “proof” of \(B\) obtained by β-normalizing \(\vdash t[u/x] : B\).

**Remark 4.45** (Extension to Classical Logic). With further enrichment of the simply-typed \(\lambda\)-calculus, the Curry-Howard correspondence actually extends to classical propositional logic, see [SU06, §6] (also [AC98, §8.5]). Beware that the resulting correspondence does not extend Tab. 2. In particular, interpreting (classical) disjunctions as sum types requires to switch to a call-by-value \(\lambda\)-calculus.

---

10See e.g. [Awo10, §6.3] and [LS86, Ex. I.7.4 & §I.8] (outside the scope of this course).

11See [LS86, §I.8] and [Sel01] (outside the scope of this course).
5. Normalization for Simple Types

5.1. Introduction

In the case of the simply typed λ-calculus, most normalization properties are provable by direct induction on typed terms (see e.g. [SU06, §3.5]). However, these proofs are often difficult (and sometime impossible) to generalize.

We are going to discuss proofs using a method called reducibility. Reducibility applies to (much) stronger type systems than simple types; it is actually the only known way to prove the termination of any type system extending Girard’s System F\(^{12}\) §9. Besides [SU06, §11], see [GLT89, Bar92, Kri93], as well as [Pie02, §23].

The reducibility method follows a general pattern issued from realizability. Realizability in particular gives (classes of) models of higher-order arithmetic and set theory, in intuitionistic settings as well as in classical ones. It is even possible to validate axioms compatible with intuitionistic logic but which are classically false (§8.3)! See [TvD88a, Chap. 4, §4] and also [Kri09, Kri01].

Another version of realizability, called logical relations, is a widespread tool to prove various properties of (models of) higher-order functional programming languages.\(^{13}\)

We present the basic mechanisms of the technique, and illustrate it with proofs of normalization results of increasing strengths. We introduce the ingredients steps by steps. After some notational preliminaries (§5.2), we begin in §5.3 with a proof of the Disjunction Property (in the form of Cor. 4.34, §4.4.4). In §5.4, we strengthen this argument to a proof of Weak Normalization for the Weak Head Reduction (to be defined in §5.3.1). We finally present in §5.5 the adaptations needed in order to obtain a proof of Strong Normalization for the Full Strong Reduction.

Standard references include [GLT89, Bar92, Kri93].

5.2. Notational Preliminaries

The reference λ-calculus for this §5 is the simply-typed λ-calculus with sums and products described in §4.4.3. Extending §3.2.1 (actually Notation 3.7, §3.2.4) we write Λ for the set of extended λ-terms of §4.4.3 (modulo α-conversion). Recall that \(X\) is the set of variables for λ-terms.

We generalize the operation of capture-avoiding substitution (Def. 3.8, §3.3.1) to the following notion of simultaneous capture-avoiding substitution.

**Definition 5.1 (Simultaneous Substitution).** Let \(σ\) be a partial function \(X \rightarrow Λ\). The **simultaneous capture-avoiding substitution** \(σt\) is defined by induction on \(t\) in Fig. 8, where \(FV(img(σ))\) stands for \(\bigcup_{x \in \text{dom}(σ)} FV(σ(x))\).

**Notation 5.2.**

1. \(Λ : X \rightarrow Λ\) as in Def. 5.1 is often called a **substitution**.

---

\(^{12}\)A.k.a. Reynolds’ Polymorphic λ-Calculus.

\(^{13}\)See e.g. [AC98, §4.5] (outside the scope of this course).
5. Normalization for Simple Types

\[
x\sigma := \sigma(x) \quad \text{if } x \in \text{dom}(\sigma)
\]

\[
x\sigma := x \quad \text{if } x \notin \text{dom}(\sigma)
\]

\[
(\lambda x.t)\sigma := \lambda x.t\sigma \quad \text{if } x \notin \text{dom}(\sigma) \cup \text{FV}(\text{img}(\sigma))
\]

\[
(tu)\sigma := t\sigma u\sigma
\]

\[
()\sigma := ()
\]

\[
(t,u)\sigma := (t\sigma,u\sigma)
\]

\[
(\pi_i t)\sigma := \pi_i t\sigma \quad \text{for } i = 1,2
\]

\[
(\text{in}_i t)\sigma := \text{in}_i t\sigma \quad \text{for } i = 1,2
\]

if \(x_1,x_2 \notin \text{dom}(\sigma) \cup \text{FV}(\text{img}(\sigma))\),

\[
\text{case } t \{ \text{in}_1 x_1 \mapsto u_1 \mid \text{in}_2 x_2 \mapsto u_2 \}\sigma := \text{case } t\sigma \{ \text{in}_1 x_1 \mapsto u_1\sigma \mid \text{in}_2 x_2 \mapsto u_2\sigma \}
\]

\[
\text{case}_\bot t \{ \}\sigma := \text{case}_\bot t\sigma \{ \}
\]

Figure 8: Simultaneous Capture-Avoiding Substitution.

(2) When \(x \notin \text{dom}(\sigma)\), we write \(\sigma[u/x]\) for the substitution taking \(x\) to \(u\) and equal to \(\sigma\) everywhere else.

Note that \(t(\sigma[u/x]) = (t\sigma)[u/x]\) if \(x \notin \text{FV}(\text{img}(\sigma))\); we can thus unambiguously write \(t\sigma[u/x]\) in this case.

(3) When \(\text{dom}(\sigma) = \{x_1,\ldots,x_n\}\) we often write \([\sigma(x_1)/x_1,\ldots,\sigma(x_n)/x_n]\) for \(\sigma\), and thus \(t[\sigma(x_1)/x_1,\ldots,\sigma(x_n)/x_n]\) for \(t\sigma\).

In particular, \([u_1/x_1,\ldots,u_n/x_n]\) stands for the substitution of domain \(\{x_1,\ldots,x_n\}\) which takes \(x_i\) to \(u_i\).

Notation 5.3 (Types). For this §5, we write \(Ty\) for the set of simple types with sums and products (§4.4.3), with base types \(\kappa\) ranging over a determined set \(K\).

Finally, we use the notions related to normalization introduced in Def. 3.33 (§3.4.3).

5.3. A First Normalization Result: The Disjunction Property

In this §5.3, we present the basic mechanism of the reducibility technique, and illustrate it with a proof of the Disjunction Property, in the form of Cor. 4.34 (§4.4.4). See Cor. 5.11 (§5.3.3) below.

5.3.1. Weak Head Reduction

We begin by noting that in order to get Lem. 4.33 (4.4.4) on Closed Typed Normal Forms, we actually do not need the full strong reduction relation \(\triangleright_\beta\) but only the weaker (and simpler) weak head reduction. This shall greatly simplify the proof of the disjunction property.

Recall the basic reduction relation \(\triangleright_0\) from Fig. 5 (§4.4.3). If we inspect the proof of Lem. 4.33, we remark that beside \(\triangleright_0 \subseteq \triangleright_\beta\), we only use the closure of \(\triangleright_\beta\) under the
5. Normalization for Simple Types

following rules:

\[
\begin{align*}
\frac{u \triangleright_\beta u'}{u \cdot v \triangleright_\beta u' \cdot v} & \quad \frac{u \triangleright_\beta u'}{\pi_1 u \triangleright_\beta \pi_1 u'} & \quad \frac{u \triangleright_\beta u'}{\text{case}_1 u \{\} \triangleright_\beta \text{case}_1 u' \{\}} \\
\frac{u \triangleright_\beta u'}{\text{case} u \{\text{in}_1 x \mapsto v \mid \text{in}_2 x \mapsto w\} \triangleright_\beta \text{case} u' \{\text{in}_1 x \mapsto v \mid \text{in}_2 x \mapsto w\}}
\end{align*}
\]

The least relation containing \(\triangleright_0\) and closed under the above rules is the \textbf{weak head reduction}. For the following, it will be convenient to define it by “plugging” the basic reduction \(\triangleright_0\) into some term-contexts of a very constrained form, ensuring that reduction steps can only occur in weak head position. These contexts are called \textbf{elimination contexts}. They are the terms with a hole (noted \([\ ]\)) inductively defined as follows:

\[
E[\ ] \in \text{Elim} ::= [\ ] \mid E[\ ] t \mid \pi_1 E[\ ] \mid \pi_2 E[\ ] \\
\quad \mid \text{case } E[\ ] \{\text{in}_1 x \mapsto u \mid \text{in}_2 x \mapsto v\} \mid \text{case } E[\ ] \{\}
\]

We write \(E[t]\) for the term obtained by substituting \(t\) for the (unique occurrence of) the hole \([\ ]\) in \(E[\ ]\). Note that elimination contexts are stable by composition: if \(E[\ ], F[\ ] \in \text{Elim}\), then \(E[F[\ ]] \in \text{Elim}\).

\textbf{Definition 5.4 (Weak Head Reduction).} The relation \(\triangleright_{wh}\) of \textbf{weak head reduction} is defined as \(t \triangleright_{wh} u\) if and only if there is an elimination context \(E[\ ]\) and terms \(v, w\) such that \(t = E[v]\), \(u = E[w]\) and \(v \triangleright_0 w\).

A direct consequence of the definition is that if \(t \triangleright_{wh} u\), then we also have \(E[t] \triangleright_{wh} E[u]\) for all elimination context \(E[\ ]\). This leads to an analogue of Lem. 4.33 for the closed normal forms of \(\triangleright_{wh}\). A \textbf{weak head normal form} is a normal form for \(\triangleright_{wh}\).

\textbf{Lemma 5.5 (Closed Normal Forms).} If \(t\) is a closed typable term in weak head normal form, then \(t\) is of one of the following forms:

\[
\lambda x. u \quad \langle\rangle \quad \langle u, v\rangle \quad \text{in}_1 u \quad \text{in}_2 u
\]

\textbf{Proof. Exercise!}\]

\textbf{Remark 5.6.} The weak head reduction a “call-by-name” reduction strategy since arguments of \(\beta\)-redexes are only evaluated when they appear in head position, and never before contracting the \(\beta\)-redex. This is also a strategy for \textbf{weak} reduction: no redex is contracted under an abstraction. Such reduction strategies are very useful in practice, since they can be easily implemented with abstract machines.

5.3.2. Type Interpretations and Adequacy

The general idea is the following: Assume that we want to prove that all typable terms \(\vdash t : T\) satisfy a given property \(P\). This property may be difficult to prove by a direct induction on the term structure or on the typing derivations. This is typically the case of termination.
Now, think of $P$ as a subset of $\Lambda$, i.e. $P \subseteq \Lambda$. The idea to find a map $\lfloor - \rfloor$, mapping each type $T \in Ty$ to a set of terms satisfying $P$: $\lfloor T \rfloor \subseteq P$. If we achieve to show that $\vdash t : T$ implies $t \in \lfloor T \rfloor$, then we are done. We call $\lfloor - \rfloor : Ty \rightarrow P(\Lambda)$ a type interpretation. If $\vdash t : T$ implies $t \in \lfloor T \rfloor$, then $\lfloor - \rfloor$ will be called adequate.

**Definition 5.7 (Adequacy).** Let $\lfloor - \rfloor : Ty \rightarrow P(\Lambda)$.

1. Given a substitution $\sigma$ and a typing context $\mathcal{E}$, we write $\sigma \models_{\lfloor - \rfloor} \mathcal{E}$ if $\text{dom}(\mathcal{E}) \subseteq \text{dom}(\sigma)$ and $\sigma(x) \in \lfloor T \rfloor$ for all $(x : T) \in \mathcal{E}$.

2. A type interpretation $\lfloor - \rfloor$ is **adequate** if $t\sigma \in \lfloor T \rfloor$ whenever $\mathcal{E} \vdash t : T$ and $\sigma \models_{\lfloor - \rfloor} \mathcal{E}$.

Let us now discuss some general conditions to get an adequate type interpretation. In most (if not all) cases, type interpretations $\lfloor - \rfloor : Ty \rightarrow P(\Lambda)$ are defined by induction on the type structure, and adequacy is proved by induction on typing derivations.

Without making any assumption on $\lfloor - \rfloor$, we can already look at what happens in the base case of an adequacy proof. Consider thus the case of the rule $(\text{Var})$ $(x : T) \in \mathcal{E} \vdash x : T$.

But if $\sigma \models_{\lfloor - \rfloor} \mathcal{E}$ then by definition we have $\sigma(x) \in \lfloor T \rfloor$. Hence, any type interpretation validates the $(\text{Var})$ rule.

All other typing rules involve a type constructor. Let us be a bit more precise about $\lfloor - \rfloor$. Assume that each base type $\kappa \in K$ has a given interpretation $\lfloor \kappa \rfloor \in P(\Lambda)$. Assume moreover that we have attributed an interpretation $\lfloor \text{unit} \rfloor$ and $\lfloor \text{void} \rfloor$ to the unit types $\text{unit}$ and $\text{void}$. The interpretation of an arbitrary type is then inductively defined using an operator on $P(\Lambda)$ per connective. The following operators $\sqcap$ and $\otimes$ correspond to the type constructors $(- \rightarrow (-)$ and $(-) \times (-)$.

**Definition 5.8.** Given $A, B \in P(\Lambda)$, let

\[\begin{align*}
A \sqcap B & \quad := \{ t \mid (\forall u \in A)(tu \in B) \} \\
A \otimes B & \quad := \{ t \mid \pi_1 t \in A \text{ and } \pi_2 t \in B \}
\end{align*}\]

Assume now that $\lfloor - \rfloor$ is such that for any types $T, U$, we have:

\[\begin{align*}
\lfloor U \rightarrow T \rfloor & \quad = \lfloor U \rfloor \sqcap \lfloor T \rfloor \\
\lfloor T \times U \rfloor & \quad = \lfloor T \rfloor \otimes \lfloor U \rfloor
\end{align*}\]

It is not difficult to see that such an interpretation validates the elimination rules of $\rightarrow$ and $\times$. Consider for instance the case of

\[\begin{align*}
(\rightarrow\text{E}) & \quad \frac{\mathcal{E} \vdash t : U \rightarrow T \quad \mathcal{E} \vdash u : U}{\mathcal{E} \vdash tu : T}
\end{align*}\]

Let $\sigma \models_{\lfloor - \rfloor} \mathcal{E}$. By induction hypothesis $t\sigma \in \lfloor U \rfloor \sqcap \lfloor T \rfloor$ and $u\sigma \in \lfloor U \rfloor$, and by definition of $\sqcap$ we get $(t\sigma)(u\sigma) \in \lfloor T \rfloor$. Then we are done since $(tu)\sigma = (t\sigma)(u\sigma)$. 57
5. Normalization for Simple Types

There is however a difficulty with the introduction rules. Consider for instance

\[(\rightarrow I) \quad \frac{E, x : U \vdash t : T}{E \vdash \lambda x.t : U \rightarrow T}\]

Let \(\sigma \models x \notin \text{FV(img}(\sigma))\). We thus have \((\lambda x.t)\sigma = \lambda x.(t\sigma)\). By definition of \(\Box\rightarrow\), we must show that \((\lambda x.(t\sigma))u \in [T]\) whenever \(u \in [U]\).

Let \(u \in [U]\). By induction hypothesis, we have \((t\sigma)[u/x] = t\sigma[u/x] \in [T]\). Hence, in order to conclude, we would like to deduce \((t\sigma)[u/x] \in [T]\) from \((\lambda x.t\sigma)u \in [T]\).

A slight generalization would lead us to require that for all \(T \in Ty\), \([T]\) satisfies the following invariant:

(stability by expansion) if \(u \in [T]\) and \(t \triangleright_0 u\) then \(t \in [T]\).

Since \([-\![\_]\]-] is defined by induction on types, we would like this invariant to be preserved by \(\Box\rightarrow\) and \(\Box\). Consider for instance the case of \(\Box\rightarrow\), and let us look at what we need to impose on \(A, B \in P(\Lambda)\) in order to ensure the stability by expansion of \(A \Box\rightarrow B\). Let \(u \in A \Box\rightarrow B\) and \(t \triangleright_0 u\). We have to show that for all \(v \in A\), we have \(tv \in B\) under the assumption that \(uv \in B\). In other word, \(B\) must be stable by expansion not only for \(\triangleright_0\), but also for a relation \(\triangleright\) containing \(\triangleright_0\) and closed under the context rule

\[
\frac{t \triangleright u}{tv \triangleright uv}
\]

By iterating the argument, we would (almost) arrive at the following: for all type \(T\), we ask \([T]\) to be stable by weak head expansion:

- \((WHE)\) if \(u \in [T]\) and \(t \triangleright_{wh} u\) then \(t \in [T]\).

5.3.3. Proof of the Disjunction Property

In order to complete the definition of an adequate type interpretation, we have to devise interpretations for the unit types \texttt{unit} and \texttt{void}, as well as for the sum types constructor \((-) + (-)\). For the moment, assume that

\[
[T + U] = [T] \oplus [U] \quad \text{[unit]} = 1 \quad \text{[void]} = 0
\]

where \(\oplus\), \(1\) and \(0\) are defined as:

\[
A \oplus B := \{ t \mid (\exists u)(t \triangleright_{wh}^* (\text{in}_1 u) \land u \in A) \lor (\exists u)(t \triangleright_{wh}^* (\text{in}_2 u) \land u \in B)\}
\]

\[
1 := \{ t \mid t \triangleright_{wh}^* \emptyset \}
\]

\[
0 := \emptyset
\]

These definitions follow a pattern different from what we have already seen: they are by introduction (or positive) rather than by elimination (or negative). We are thus in a somehow dual situation w.r.t. the cases of \(\Box\rightarrow\) and \(\Box\). In particular, it is easy to see that \(\oplus\) and \(1\) directly validate the introduction rules of \((-) + (-)\) and \texttt{unit}, while we rely on \((WHE)\) for the elimination rule of \((-) + (-)\):
Proposition 5.9. Let $A, B, C \in \mathcal{P}(\Lambda)$ such that $C$ satisfies ($\mathcal{WHE}$). Let $t, v, w$ such that $t \in A \oplus B$, $v[u/x] \in C$ for all $u \in A$ and $w[u/x] \in C$ for all $u \in B$. Then $\text{case } t \{(\text{in}_1 x \mapsto v \mid \text{in}_2 x \mapsto w)\} \in C$.

Proof. Exercise! \qed

Consider now the case of $0$. It trivially satisfies ($\mathcal{WHE}$). Let us see that it also validates the elimination rule of void

$$\text{(void-E)} \quad \frac{\mathcal{E} \vdash t: \text{void}}{\mathcal{E} \vdash \text{case } t \{\} : T}$$

Let $\sigma \models \Gamma \mathcal{E}$. We have to show that $\text{case } (t\sigma \{\}) \in \llbracket T \rrbracket$, while we have no assumption on $T$. It can be for instance void, while $\llbracket \text{void} \rrbracket = \emptyset$. But the induction hypothesis tells us that $t\sigma \in \llbracket \text{void} \rrbracket = \emptyset$. This is a contradiction, from which follows anything; in particular $\text{case } (t\sigma \{\}) \in \llbracket T \rrbracket$ for any type $T$.

Putting everything together, we have the following:

Theorem 5.10 (Adequacy). Let $\llbracket - \rrbracket$ be a type interpretation such that

(i) $\llbracket \kappa \rrbracket$ satisfies ($\mathcal{WHE}$) for all $\kappa \in K$, and

(ii) $\llbracket \text{unit} \rrbracket = 1$ and $\llbracket \text{void} \rrbracket = 0$, and

(iii) for all types $T, U$,

$$\llbracket U \to T \rrbracket = \llbracket U \rrbracket \rightarrow \llbracket T \rrbracket \quad \llbracket T \times U \rrbracket = \llbracket T \rrbracket \otimes \llbracket U \rrbracket \quad \llbracket T + U \rrbracket = \llbracket T \rrbracket \oplus \llbracket U \rrbracket$$

Then,

(1) for all type $T$, $\llbracket T \rrbracket$ satisfies ($\mathcal{WHE}$), and

(2) $\llbracket - \rrbracket$ is adequate.

Proof. Exercise! \qed

Let us now look at what can be said from Thm. 5.10. At first sight, it may seem that we have imposed very few properties on $\llbracket - \rrbracket$. It is nevertheless enough to obtain the Disjunction Property.

Corollary 5.11 (Cor. 4.34 (§4.4.4)). In the simply-typed $\lambda$-calculus with sums and products,

(1) there is no $\lambda$-term $t$ such that $\vdash t : \text{void}$;

(2) if $\vdash t : T_1 + T_2$ then there are some $i \in \{1, 2\}$ and some $\lambda$-term $u_i$ such that $t \triangleright^* \text{in}_i u_i$ and $\vdash u_i : T_i$.

Proof. Exercise! \qed

We thus have proved the Disjunction Property. However, Thm. 5.10 gives no information on the normalization of typed terms of arbitrary types.
5. Normalization for Simple Types

5.4. Reducibility Candidates

In this section, we adapt the basic material of §5.3 to prove (weak) normalization of typed terms of arbitrary types. To keep things simple, we consider the weak normalization of weak head reduction $\triangleright_{wh}$.

**Warning 5.12.** In this §5.4, by weak normalization we mean weak normalization w.r.t. $\triangleright_{wh}$. Write $\mathcal{WN}$ for the set of weakly normalizable terms w.r.t. $\triangleright_{wh}$.

In order to show that $\vdash t : T$ implies $t \in \mathcal{WN}$, we only have to find a type interpretation $\llbracket - \rrbracket$ such that $\llbracket T \rrbracket \subseteq \mathcal{WN}$ for all type $T$. First, note that requiring $\llbracket T \rrbracket \subseteq \mathcal{WN}$ does not conflict with $(\mathcal{WHE})$.

**Lemma 5.13.** Let $A \subseteq \mathcal{WN}$. Then $\{ t \mid \exists (u \in A)(t \triangleright^*_{wh} u) \}$ is the least subset of $\mathcal{WN}$ which contains $A$ and satisfies $(\mathcal{WHE})$.

Consider now a type interpretation $\llbracket - \rrbracket$, which satisfies the hypotheses of Thm. 5.10 and such that moreover $\llbracket \kappa \rrbracket \subseteq \mathcal{WN}$ for all $\kappa$. Note that $\llbracket \text{unit} \rrbracket, \llbracket \text{void} \rrbracket \subseteq \mathcal{WN}$.

Let us check whether the requirement $\llbracket T \rrbracket \subseteq \mathcal{WN}$ is preserved by the (interpretations of the) type constructors. The case of $\oplus$ is trivial since we have $A \oplus B \subseteq \mathcal{WN}$ for all $A, B \in \mathcal{P}(\Lambda)$. Moreover, it is not difficult to see that $A \triangleright B \subseteq \mathcal{WN}$ provided $A, B \subseteq \mathcal{WN}$.

**Exercise 5.14.** Show that $A \triangleright B \subseteq \mathcal{WN}$ whenever $A, B \subseteq \mathcal{WN}$. What property of $\triangleright_{wh}$ do you use?

However, there is a problem with $\triangleleft$ since

$$0 \triangleleft A = \{ t \mid (\forall u)(u \in \emptyset \implies tu \in A) \} = \Lambda$$

More generally,

- in presence possibly empty types interpretations, there is no invariant preserved by $\triangleleft$.

We thus have to ensure that $\llbracket - \rrbracket$ maps types to non-empty sets of terms. In the case of normalization properties, one usually requires $\llbracket T \rrbracket$ to contain variables. Similarly as with the weak expansion requirement discussed in §5.3.2, in order to ensure that this invariant is preserved by the (interpretations of) type constructors, we formulate it as follows:

- $E[x] \in \llbracket T \rrbracket$ for all $E[\ ] \in \text{Elim}$ and all $x \in X$.

This invariant is designed to be preserved by the negative interpretations $\triangleleft$ and $\triangleright$. It is however not satisfied by the positive interpretations $0, 1$ and $\oplus$. These interpretations could be adapted in order to satisfy our requirement. But we prefer to take the opportunity to define their respective negative counterparts $\bot, \top$ and $\triangleright$. 

60
Consider the case of \((-\) + \((-\). In order to get a negative interpretation, we follow our methodology and look at the elimination rule
\[
\begin{array}{c}
\frac{E \vdash t : T_1 + T_2 \quad E, x : T_1 \vdash u_1 : U \quad E, x : T_2 \vdash u_2 : U}{E \vdash \text{case } t \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto u_2 \} : U}
\end{array}
\]
There is a difficulty here: the type $U$ to which case eliminates a term $t : T_1 + T_2$ has in general no relation with $T_1$ nor $T_2$. A tentative definition of $A \⊞ B$ could be to take the set of all terms $t$ such that
\[
\forall T \in \text{Ty}, \quad \forall u \text{ s.t. } u[w/x] \in [T] \text{ whenever } w \in A, \\
\forall v \text{ s.t. } v[w/x] \in [T] \text{ whenever } w \in B,
\]
we have \(\text{case } t \{ \text{in}_1 x \mapsto u \mid \text{in}_2 x \mapsto v \} \in [T]\)
However, such a definition would not be well-formed since the interpretation $[T]$ may itself use $\⊞$.
The standard way to get rid of this circularity is to define $\⊞$ by quantifying not over types, but rather over a predefined family of "candidate interpretations". The family presented here is the family of "saturated sets".

**Definition 5.15 (Saturated Sets).** The set $\mathcal{SAT}_{\text{WN}}$ of $\text{WN}$-saturated sets is the set of all $A \subseteq \text{WN}$ such that
\[
\begin{align*}
(i) & \quad E[x] \in A \text{ for all } E[\cdot] \in \text{Elim}, \text{ and} \\
(ii) & \quad E[t] \in A \text{ if } t \triangleright_0 u \text{ for some } E[u] \in A.
\end{align*}
\]
We first check that the family $\mathcal{SAT}_{\text{WN}}$ is not empty.

**Lemma 5.16.** The set $\mathcal{SAT}_{\text{WN}}$ is a complete lattice w.r.t. inclusion, whose top element is $\top := \text{WN}$ and whose least element is $\bot := \{ t \mid (\exists E[\cdot], x)(t \triangleright_0^* E[x]) \}$. The complete lattice structure of $\mathcal{SAT}_{\text{WN}}$ gives us negative interpretations of $\text{void}$ and $\text{unit}$.

- We take the negative interpretation of $\text{void}$ to be $\bot$. Note that
\[
\bot = \{ t \mid (\forall A \in \mathcal{SAT}_{\text{WN}}) (\text{case}_\bot t \{ \} \in A) \}
\]
PROOF. Exercise!

Hence, if $t \in \bot$, then we have $\text{case}_\bot t \{ \} \in A$ for any $A \in \mathcal{SAT}_{\text{WN}}$. It follows that $[\text{void}] = \bot$ validates the rule (void-E).

- Similarly, we take the negative interpretation of $\text{unit}$ to be $\top$. It validates (unit-I) since $\{ \} \in \text{WN}$.

The negative interpretation of $(-) + (-)$ is defined as follows.

61
5. Normalization for Simple Types

Definition 5.17. Given \( A, B \in P(\Lambda) \), let \( A \oplus_{WN} B \) be the set of all terms \( t \) such that

\[
\forall C \in SAT_{WN}, \quad \forall u \text{ s.t. } u[w/x] \in C \text{ whenever } w \in A, \quad \forall v \text{ s.t. } v[w/x] \in C \text{ whenever } w \in B,
\]

we have \( \text{case } t \{ \text{in}_1 x \mapsto u \mid \text{in}_2 x \mapsto v \} \in C \).

Note that \( \oplus_{WN} \) depends on \( SAT_{WN} \). Our connectives preserve saturated sets.

Lemma 5.18. Let \( A, B \in SAT_{WN} \). Then

\[
A \sqsupset B, A \otimes B, A \oplus_{WN} B \in SAT_{WN}
\]

We thus get the analogue of the Adequacy Theorem 5.10.

Theorem 5.19 (Adequacy). Let \([\cdot]\) be a type interpretation such that

(i) \([\kappa]\) \( \in SAT_{WN} \) for all \( \kappa \in \mathcal{K} \), and

(ii) \([\text{unit}] = \top \) and \([\text{void}] = \bot \), and

(iii) for all types \( T, U \),

\[
[U \to T] = [U] \cdot [T] \quad [T \times U] = [T] \otimes [U] \quad [T + U] = [T] \oplus_{WN} [U]
\]

Then,

(1) \([T]\) \( \in SAT_{WN} \) for all type \( T \), and

(2) \([\cdot]\) is adequate.

Proof. Exercise!

The weak normalization of typable terms immediately follows.

Corollary 5.20 (Weak Normalization). If \( \mathcal{E} \vdash t : T \) then \( t \in WN \).

Proof. Exercise!

5.5. Strong Normalization

We now extend the material of §5.4 in order to get the strong normalization of well-typed terms. We begin in §5.5.1 and §5.5.2 with combinatorial properties on the notion of strong normalization. The (then direct) adaptations to Saturated Sets and Adequacy are discussed in §5.5.3.
5. Normalization for Simple Types

5.5.1. Inductive Definition of Strong Normalization

We momentarily step back from $\lambda$-terms to Abstract Reduction Systems (ARS's, §3.4).

Let $(A, \triangleright)$ be an ARS. We are interested in giving an inductive description of the strongly normalizing elements of $A$. Recall that according to Def. 3.33 (§3.4.3), $a \in A$ is strongly normalizing if there is no infinite sequence $(a_i)_{i \in \mathbb{N}}$ of elements of $A$ such that $a_0 = a$ and $a_i \triangleright a_{i+1}$ for all $i \in \mathbb{N}$. In the following it is convenient to say that an infinite reduction sequence from $a \in A$ is an infinite sequence $(a_i)_{i \in \mathbb{N}}$ of elements of $A$ such that $a_0 = a$ and $a_i \triangleright a_{i+1}$ for all $i \in \mathbb{N}$.

**Definition 5.21.** Let $SN$ be the least subset of $A$ such that for all $a \in A$ we have

$$ (\forall b \in A)(a \triangleright b \implies b \in SN) \implies a \in SN $$

Note that $SN$ can be characterized as the least subset of $A$ closed under the rule

$$ (\forall b \in A)(a \triangleright b \implies b \in SN) $$

$$ a \in SN $$

It is direct to see that all $a \in SN$ are strongly normalizing.

**Lemma 5.22.** If $a \in SN$ the $a$ strongly normalizing.

**Proof.** Exercise! □

Note that the proof of Lem. 5.22 is constructive, since it proves the negative statement “there is no infinite reduction sequence [...]”.

On the other hand, the converse of Lem. 5.22 is not constructive.

**Proposition 5.23.** Given an ARS $(A, \triangleright)$ and $a \in A$, we have $a \in SN$ if and only if $a$ is strongly normalizing.

**Proof.** We already know from Lem. 5.22 that $a$ is strongly normalizing when $a \in SN$. For the converse, note that for all $a \notin SN$, there is some $b \notin SN$ such that $a \triangleright b$. Hence if $a \notin SN$ there exists an infinite reduction sequence from $a$. □

The proof of Prop. 5.23 relies on classical logic (as we reasoned by contradiction to prove the positive statement “$a \in SN$”) moreover using a form of the Axiom of Choice to ensure the existence of the infinite reduction sequence.\(^{14}\)

**Notation 5.24.** For the remaining of this §5.5, we let $SN$ stand for strong normalization w.r.t. $\beta$-reduction.

\(^{14}\)Actually an instance of **Dependent Choices**, see *e.g.* [TvD88a, Chap. 4, §2.3].
5. Normalization for Simple Types

5.5.2. Strong Normalization and Weak Head Reduction

The adaptation of the saturation clauses of Def. 5.15 to strong normalization is straightforward once we know how to connect strong normalization w.r.t. $\beta$ with weak head expansion.

The connection is provided by the two following lemmas, and is best expressed by using a notion of tuple reduction.

Notation 5.25. Write $(t_1, \ldots, t_n) \triangleright_{\beta} (u_1, \ldots, u_n)$ when there is some $i \in \{1, \ldots, n\}$ such that $t_i \triangleright_{\beta} u_i$ and $t_j = u_j$ for all $j \neq i$.

Let us explain the idea in the case of the pure $\lambda$-calculus. We would like to adapt Def. 5.15 to strong normalization. First, for a set $A \in \mathcal{P}(\Lambda)$ to be saturated, we shall ask that $A$ contains only strongly normalizing terms: $A \subseteq SN$. Now, we have to adapt the two clauses Def. 5.15, in order to avoid conflict with the invariant $A \subseteq SN$. The first clause

- $E[x] \in A$ for all $E[\ ] \in \text{Elim}$

is obviously adapted to

- $E[x] \in A$ for all $E[\ ] \in \text{Elim} \cap SN$.

Consider now the second clause:

- $E[(\lambda x.t)u] \in A$ if $E[t[u/x]] \in A$.

This clause is problematic only in the following case: Assume that the variable $x$ does not occur free in $t$ and that $u$ is not normalizable. Then $E[t[u/x]] = E[t]$ can be strongly normalizing while $E[(\lambda x.t)u]$ is not. This is easily patched by asking $u$ to be strongly normalizing:

- $E[(\lambda x.t)u] \in A$ if $E[t[u/x]] \in A$ and $u \in SN$.

This clause is correct, in the sense that $E[(\lambda x.t)u]$ is strongly normalizing if both $E[t[u/x]]$ and $u$ are.

Let us look at this more precisely. Assume that $E[t[u/x]] \in SN$ and $u \in SN$. According to the definition of $SN$, we must show that for all $v$, if $E[(\lambda x.t)u] \triangleright_{\beta} v$ then $v \in SN$. Now, since we are in the pure $\lambda$-calculus, $E[\ ]$ is of the form $[ ]t_1 \ldots t_n$. Note that $t, u, t_1, \ldots, t_n \in SN$. The different possibilities for $v$ can be depicted as follows:

$$(\lambda x.t)u_1 \ldots t_n \triangleright_{\beta} t[u/x]t_1 \ldots t_n$$

$$\downarrow \triangleright_{\beta}^*$$

$$(\lambda x.t')u't'_1 \ldots t'_n \triangleright_{\beta} t'[u'/x]t'_1 \ldots t'_n$$

Hence, there are schematically two possibilities for $v$. If $v = t[u/x]t_1 \ldots t_n$ then we are done. Otherwise, $v$ is of the form $(\lambda x.t')u't'_1 \ldots t'_n$ with $(t, u, t_1, \ldots, t_n) \triangleright_{\beta} (t', u', t'_1, \ldots, t'_n)$.  

64
5. Normalization for Simple Types

In this case, we still have \( t', u', t'_1, \ldots, t'_n \in SN \) and \( t'[u'/x]t'_1 \ldots t'_n \in SN \). This suggests to reason by induction on \( t, u, t_1, \ldots, t_n \in SN \).

More generally, we can show by induction on \( E[ ] \), \( t, u \in SN \) that

- \( E[(\lambda x.t)u] \in SN \) if \( E[t[u/x]] \in SN \) and \( u \in SN \).

This reasoning easily generalizes to the other term constructors, as stated in the two following lemmas.

**Lemma 5.26** (Weak Standardization). Let \( E[ ] \in \text{Elim} \).

1. If \( E[(\lambda x.t)u] \triangleright_{\beta} v \), then either \( v = E[t[u/x]] \) or \( t \) is of the form \( E'[ (\lambda x.t')u'] \) with \( E[ ], t, u \triangleright_{\beta} (E'[ ], t', u') \).

2. Let \( i \in \{1, 2\} \). If \( E[\pi_i(t_1, t_2)] \triangleright_{\beta} v \), then either \( v = E[t] \) or \( t \) is of the form \( E'[\pi_i(t'_1, t'_2)] \) with \( E[ ], t_1, t_2 \triangleright_{\beta} (E'[ ], t'_1, t'_2) \).

3. Let \( i \in \{1, 2\} \). If \( E[\text{case } (\text{in}_i \ t) \{ \text{in}_1 x \mapsto u_1 \ | \ \text{in}_2 x \mapsto u_2 \}] \triangleright_{\beta} v \), then either \( v = E[u_i[t/x]] \) or \( t \) is of the form \( E[\text{case } (\text{in}_i \ t') \{ \text{in}_1 x \mapsto u'_1 \ | \ \text{in}_2 x \mapsto u'_2 \}] \) with \( E[ ], t, u_1, u_2 \triangleright_{\beta} (E[ ], t', u'_1, u'_2) \).

**Proof.** Exercise! \( \square \)

The Weak Standardization Lemma 5.26 exhibits a very good behaviour of weak head expansion w.r.t. strong normalization.

**Lemma 5.27** (Weak Head Expansion). Let \( E[ ] \in \text{Elim} \).

1. If \( E[t[u/x]] \in SN \) and \( u \in SN \) then \( E[(\lambda x.t)u] \in SN \).

2. Let \( i \in \{1, 2\} \). If \( E[t_i] \in SN \) and \( t_{3-i} \in SN \) then \( E[\pi_i(t_1, t_2)] \in SN \).

3. Let \( i \in \{1, 2\} \). If \( E[u_i[t/x]] \in SN \) and \( t, u_{3-i} \in SN \) then \( E[\text{case } (\text{in}_i \ t) \{ \text{in}_1 x \mapsto u_1 \ | \ \text{in}_2 \mapsto u_2 \}] \in SN \).

**Proof.** Exercise! \( \square \)

### 5.5.3. Type Interpretations and Adequacy

We can now give the adaptation of Def. 5.15 to strong normalization.

**Definition 5.28** (Saturated Sets). The set \( SAT_{SN} \) of \( SN \)-saturated sets is the set of all \( A \subseteq SN \) such that

1. \( E[x] \in A \) whenever \( E[ ] \in \text{Elim} \cap SN \), and
2. \( E[(\lambda x.t)u] \in A \) whenever \( u \in SN \) and \( E[t[u/x]] \in A \), and
3. for all \( i \in \{1, 2\} \), \( E[\pi_i(t_1, t_2)] \in A \) whenever \( t_{3-i} \in SN \) and \( E[t_i] \in A \), and
(iv) for all $i \in \{1, 2\}$, $E[\text{case } \text{in}_i t \{ \text{in}_1 x \mapsto u_1 \mid \text{in}_2 x \mapsto w_2 \}] \in A$ whenever $t, u_{3-i} \in \mathcal{SN}$ and $E[u_i[t/x]] \in A$.

The non-degeneracy of Def. 5.28 directly follows from Lem. 5.27. This leads to the analogue of Lem. 5.16.

**Lemma 5.29.** The set $\mathcal{SAT}_{\mathcal{SN}}$ is a complete lattice w.r.t. inclusion, whose top element is $\top := \mathcal{SN}$ and whose least element is $\bot := \{ t \in \mathcal{SN} \mid (\exists E[\_], x)(t \triangleright^w_{wh} E[x]) \}$.

**Proof.** Exercise! \qed

Recall that the negative interpretation of $(-) + (-)$ depends on the family of candidate interpretations over which we are quantifying. It has thus to be adapted. Given $A, B \in \mathcal{P}(\Lambda)$, let $A \boxplus_{\mathcal{SN}} B$ be the set of all terms $t$ such that

\[
\forall C \in \mathcal{SAT}_{\mathcal{SN}}, \\
\forall u \text{ s.t. } u[w/x] \in C \text{ whenever } w \in A, \\
\forall v \text{ s.t. } v[w/x] \in C \text{ whenever } w \in B,
\]

we have $\text{case } t \{ \text{in}_1 x \mapsto u \mid \text{in}_2 x \mapsto v \} \in C$.

**Lemma 5.30.** Let $A, B \in \mathcal{SAT}_{\mathcal{SN}}$. Then

\[
A \sqcup B, A \boxtimes B, A \boxplus_{\mathcal{SN}} B \in \mathcal{SAT}_{\mathcal{SN}}
\]

**Proof.** Exercise! \qed

We thus get the analogue of Adequacy Theorem 5.19.

**Theorem 5.31** (Adequacy). Let $[\_]$ be a type interpretation such that

(i) $[\kappa] \in \mathcal{SAT}_{\mathcal{SN}}$ for all $\kappa \in \mathcal{K}$, and

(ii) $[\text{unit}] = \top$ and $[\text{void}] = \bot$, and

(iii) for all types $T, U$,

\[
[U \rightarrow T] = [U] \rightarrow [T] \quad [T \times U] = [T] \boxtimes [U] \quad [T + U] = [T] \boxplus_{\mathcal{SN}} [U]
\]

Then $[\_]$ is adequate.

**Proof.** Exercise! \qed

We finally obtain the strong normalization of typable terms (Thm. 4.12, §4.2.2 and Thm. 4.31, §4.4.4).

**Theorem 5.32** (Strong Normalization). If $E \vdash t : T$ then $t \in \mathcal{SN}$.

**Proof.** Exercise! \qed
6. First-Order Predicate Logic

We now turn to first-order predicate logic.

The status of the Curry-Howard correspondence for intuitionistic first-order logic is somehow ambiguous. On the one hand, everything works (almost) perfectly well at the technical level. On the other hand, in proofs-assistants based on the Curry-Howard correspondence, the setting of dependent types is often preferred to first-order logic (see [SU06, §13] or [Uni13, §1], also Rem. 6.48, §6.3).\(^{15}\)

We shall pay special attention to the specific properties of intuitionistic first-order predicate logic (NJ\(_1\)), most notably concerning the extraction of witnesses from proofs of existential statements. Further, the already rich setting of NJ\(_1\) gives basic intuitions on constructive reasoning, and is the basis of important stronger systems, such as Intuitionistic Arithmetic (7.3) and Second-Order Logic (\(\aleph\)). Compared with dependent types, one feature of first-order logic is that it is sufficiently simple for easily stating (and proving) interesting non-trivial meta-theoretical properties (§7.3.3, §7.3.4, §8.3).

As shall see, the Curry-Howard correspondence for intuitionistic first-order logic is based on proof-terms which are in essence simply-typed, so that in particular their normalization is no more difficult than in the case of propositional logic (§5, §6.5). Besides, while they are not particularly interesting from a programming point of view, the proof-terms for NJ\(_1\) will play a crucial role in establishing the main extraction properties of the latter.

We assume a working knowledge of first-order logic (essentially covered by [vD04]). We however recall the relevant definitions and results.

6.1. Preliminaries

This §6.1 gathers definitions on many-sorted first-order logic. It essentially consists of a mild extension of [vD04, §2.2 & §2.3] (see also [SU06, §8.1 & §8.4] and [Bus98a, §2.1]).

6.1.1. First-Order Signatures

**Definition 6.1 (First-Order Signature).** A (first-order) signature \(\Sigma\) consists of

(i) a set \(\text{Sort}(\Sigma)\) of sorts (ranged over by \(\sigma, \tau, \theta, \ldots\));

(ii) a collection of (sorted) function symbols

\[
\text{Fun}(\Sigma) = \bigcup_{(\tau_1, \ldots, \tau_n; \sigma)\in\text{Sort}(\Sigma)^{n+1}} \text{Fun}(\Sigma)(\tau_1, \ldots, \tau_n; \sigma)
\]

(we sometimes write \(f : \tau_1 \times \cdots \times \tau_n \to \sigma\) for \(f \in \text{Fun}(\Sigma)(\tau_1, \ldots, \tau_n; \sigma)\));

(iii) a collection of (sorted) predicate (or relation) symbols

\[
\text{Pred}(\Sigma) = \bigcup_{(\tau_1, \ldots, \tau_n)\in\text{Sort}(\Sigma)^n} \text{Pred}(\Sigma)(\tau_1, \ldots, \tau_n)
\]

(we sometimes write \(P \subseteq \tau_1 \times \cdots \times \tau_n\) for \(P \in \text{Pred}(\Sigma)(\tau_1, \ldots, \tau_n)\)).

\(^{15}\)See also [Jac01, Hof97] (beyond the scope of this course).
6. First-Order Predicate Logic

**Notation 6.2.** Functions symbols \( c \in \text{Fun}(\Sigma)(\sigma) \) (i.e. \( \text{Fun}(\Sigma)(\tau_1, \ldots, \tau_n; \sigma) \) with \( n = 0 \)) are often called **constants**. We write \( c : \sigma \) instead of \( c : 1 \to \sigma \) (i.e. \( \tau_1 \times \cdots \times \tau_n \to \sigma \) with \( n = 0 \)).

**Definition 6.3** (First-Order Terms). Let \( \Sigma \) be a signature. Assume given a collection \( V = \bigcup_{\sigma \in \text{Sort}(\Sigma)} V(\sigma) \) of \( \Sigma \)-sorted first-order variables, where \( V(\sigma) \) (also written \( V^\sigma \)) is ranged over by \( x^\sigma, y^\sigma, z^\sigma \), etc.

(1) The set of **first-order terms** over \((\Sigma, V)\) is the collection \( \text{Ter}(\Sigma, V) = \bigcup_{\sigma \in \text{Sort}(\Sigma)} \text{Ter}(\Sigma, V)(\sigma) \) inductively defined as follows:

- for each \( x^\sigma \in V(\sigma) \), we have \( x^\sigma \in \text{Ter}(\Sigma, V)(\sigma) \);
- given \( f \in \text{Fun}(\Sigma)(\tau_1, \ldots, \tau_n; \sigma) \) and \( a_1 \in \text{Ter}(\Sigma, V)(\tau_1), \ldots, a_n \in \text{Ter}(\Sigma, V)(\tau_n) \), we have \( f(a_1, \ldots, a_n) \in \text{Ter}(\Sigma, V)(\sigma) \).

(2) The set \( \text{FV}(a) \) is defined by induction on \( a \) as follows:

- \( \text{FV}(x^\sigma) = \{x^\sigma\} \);
- \( \text{FV}(f(a_1, \ldots, a_n)) = \text{FV}(a_1) \cup \cdots \cup \text{FV}(a_n) \).

**Notation 6.4.**

(1) When \( \Sigma \) and \( V \) are understood from the context, we often write \( a^\sigma \) for \( a \in \text{Ter}(\Sigma, V)(\sigma) \).

(2) Given terms \( a^\sigma \) and \( b \) and a variable \( x^\sigma \), the **substitution** of \( x^\sigma \) by \( a^\sigma \) in \( b \), notation \( b[a^\sigma/x^\sigma] \), is defined in the obvious way.

(3) When \( \Sigma \) is one-sorted, i.e. when \( \text{Sort}(\Sigma) \) is a singleton (say \( \{\sigma\} \)), we write

- \( \text{Fun}(\Sigma)(n) \) for \( \text{Fun}(\Sigma)(\sigma, \ldots, \sigma; \sigma) \);
- \( \text{Pred}(\Sigma)(n) \) for \( \text{Pred}(\Sigma)(\sigma, \ldots, \sigma) \);
- \( x \in V \) for \( x^\sigma \in V(\sigma) \);
- \( a \in \text{Ter}(\Sigma, V) \) for \( a^\sigma \in \text{Ter}(\Sigma, V)(\sigma) \).

### 6.1.2. The Language of First-Order Predicate Logic

Let \( \Sigma \) be a first-order signature and \( V \) be a collection of \( \Sigma \)-sorted first-order variables. The formulae of first-order predicate logic over \((\Sigma, V)\) are given by the grammar:

\[
A, B ::= P(a_1, \ldots, a_n) \mid A \Rightarrow B \mid A \land B \mid A \lor B \mid \top \mid \bot \\
\mid (\forall x^\sigma) A \mid (\exists x^\sigma) A
\]

where \( P \in \text{Pred}(\Sigma)(\tau_1, \ldots, \tau_n) \) and \( a_i \in \text{Ter}(\Sigma, V)(\tau_i) \) for each \( i = 1, \ldots, n \).
The set \( \text{FV}(A) \) of free variables of \( A \) is defined by induction on \( A \) as follows:

\[
\begin{align*}
\text{FV}(P(a_1,\ldots,a_n)) & := \bigcup_{1 \leq i \leq n} \text{FV}(a_i) \\
\text{FV}(\forall x^\sigma A) & := \text{FV}(A) \setminus \{x^\sigma\} \\
\text{FV}(\exists x^\sigma A) & := \text{FV}(A) \setminus \{x^\sigma\} \\
\text{FV}(A \Rightarrow B) & := \text{FV}(A) \cup \text{FV}(B) \\
\text{FV}(A \land B) & := \text{FV}(A) \cup \text{FV}(B) \\
\text{FV}(A \lor B) & := \text{FV}(A) \cup \text{FV}(B) \\
\text{FV}(\top) & := \emptyset \\
\text{FV}(\bot) & := \emptyset
\end{align*}
\]

**Notation 6.5.**

1. A closed formula (i.e. a formula \( A \) such that \( \text{FV}(A) = \emptyset \)) is often called a **sentence**.
2. When \( \Sigma \) is one-sorted, i.e. when \( \text{Sort}(\Sigma) \) is a singleton (say \( \{\sigma\} \)), we write \( (\forall x) \) and \( (\exists x) \) for resp. \( (\forall x^\sigma) \) and \( (\exists x^\sigma) \).
3. We often write \( A(x^\sigma) \) to informally emphasize that the variable \( x^\sigma \) occurs or may occur free in the formula \( A \) (and similarly for first-order terms).

**Warning 6.6** (Variable Binding). Universal quantifiers \( (\forall x^\sigma)A \) (“for all”) and existential quantifiers \( (\exists x^\sigma)A \) (“there exists”) **bind** \( x^\sigma \) in \( A \). We thus assume that first-order formulae are quotiented by \( \alpha \)-equivalence (w.r.t. the obvious adaptation of §3.2.4).

Given a term \( b^\sigma \) and a variable \( x^\sigma \) the **capture-avoiding substitution** of \( x^\sigma \) by \( b^\sigma \) in \( A \) is defined by induction on \( A \) as follows:

\[
\begin{align*}
\top[b^\sigma/x^\sigma] & := \top \\
\bot[b^\sigma/x^\sigma] & := \bot \\
(P(a_1,\ldots,a_n))[b^\sigma/x^\sigma] & := P(a_1[b^\sigma/x^\sigma],\ldots,a_n[b^\sigma/x^\sigma]) \\
(A \Rightarrow B)[b^\sigma/x^\sigma] & := A[b^\sigma/x^\sigma] \Rightarrow B[b^\sigma/x^\sigma] \\
(A \land B)[b^\sigma/x^\sigma] & := A[b^\sigma/x^\sigma] \land B[b^\sigma/x^\sigma] \\
(A \lor B)[b^\sigma/x^\sigma] & := A[b^\sigma/x^\sigma] \lor B[b^\sigma/x^\sigma] \\
(\forall y^\tau)A[b^\sigma/x^\sigma] & := (\forall y^\tau)(A[b^\sigma/x^\sigma]) \quad \text{if } y \neq x \text{ and } y \notin \text{FV}(b) \\
(\exists y^\tau)A[b^\sigma/x^\sigma] & := (\exists y^\tau)(A[b^\sigma/x^\sigma]) \quad \text{if } y \neq x \text{ and } y \notin \text{FV}(b)
\end{align*}
\]

**Notation 6.7.** We extend the notations of §2 with the convention that quantifiers \( (\forall x^\sigma) \) and \( (\exists x^\sigma) \) have the highest priority, so that e.g. \( (\exists x^\sigma)A \land (\forall y^\tau)B \Rightarrow C \) stands for \( (((\exists x^\sigma)A) \land ((\forall y^\tau)B)) \Rightarrow C \).

### 6.1.3. Structures and Models

**Definition 6.8.** A **model** of a signature \( \Sigma \) (or **\( \Sigma \)-structure**) \( \mathcal{M} \) consists of

1. For each sort \( \sigma \in \text{Sort}(\Sigma) \), a **non-empty** set \( M(\sigma) \) (also written \( M^\sigma \), or even \( \llbracket \sigma \rrbracket \) when \( \mathcal{M} \) is clear from the context);
2. For each function symbol \( f \in \text{Fun}(\Sigma)(\tau_1,\ldots,\tau_n; \sigma) \), a function \( M(f) : M(\tau_1) \times \cdots \times M(\tau_n) \rightarrow M(\sigma) \) (we also write \( f_M \) or \( f^\mathcal{M} \) for \( M(f) \), or even \( \llbracket f \rrbracket \) when \( \mathcal{M} \) is clear from the context);
6. First-Order Predicate Logic

Given a \( \Sigma \) and a valuation \( v \), let \( \mathcal{M} \) be a \( \Sigma \)-structure. Then the satisfaction relation \( \mathcal{M}, v \models A \) is defined as follows:

- \( \mathcal{M}, v \models P(a_1, \ldots, a_n) \) if and only if \( ([a_1]v, \ldots, [a_n]v) \in [P] \)
- \( \mathcal{M}, v \models A \wedge B \) if \( \mathcal{M}, v \models A \) and \( \mathcal{M}, v \models B \)
- \( \mathcal{M}, v \models A \vee B \) if \( \mathcal{M}, v \models A \) or \( \mathcal{M}, v \models B \)
- \( \mathcal{M}, v \models A \Rightarrow B \) if \( \mathcal{M}, v \models A \) implies \( \mathcal{M}, v \models B \)
- \( \mathcal{M}, v \models (\forall \sigma)A \) if for all \( a \in \mathcal{M}(\sigma) \), \( \mathcal{M}, v[a/\sigma] \models A \)
- \( \mathcal{M}, v \models (\exists \sigma)A \) if there exists \( a \in \mathcal{M}(\sigma) \) such that \( \mathcal{M}, v[a/\sigma] \models A \)

\( \mathcal{M}, v \not\models \bot \)

Figure 9: The Satisfaction Relation \( \mathcal{M}, v \models A \).

(iii) for each predicate symbol \( P \in \text{Pred}(\Sigma)(\tau_1, \ldots, \tau_n) \), a subset \( \mathcal{M}(P) \) of \( \mathcal{M}(\tau_1) \times \cdots \times \mathcal{M}(\tau_n) \) (we also write \( P_\mathcal{M} \) or \( P^\mathcal{M} \) for \( \mathcal{M}(P) \), or even \([P]\) when \( \mathcal{M} \) is clear from the context).

Remark 6.9. A constant \( c \in \text{Fun}(\Sigma)(\sigma) \) is interpreted as a function \( \mathcal{M}(c) : 1 \to \mathcal{M}(\sigma) \) (where \( 1 = \{\bullet\} \)), equivalently as an element \( \mathcal{M}(c)(\bullet) \in \mathcal{M}(\sigma) \) that we still denote \( \mathcal{M}(c) \).

Notation 6.10. When \( \Sigma \) is one-sorted, i.e. when \( \text{Sort}(\Sigma) \) is a singleton (say \( \{\sigma\} \) ), we write \( \mathcal{M} \) for \( \mathcal{M}(\sigma) \).

The notion of satisfaction of a formula \( A \) in a model \( \mathcal{M} \) under a valuation \( v \) (notation \( \mathcal{M}, v \models A \)) is standard. First, by a valuation \( v \) we mean a collection \( (v^\sigma)_{\sigma \in \text{Sort}(\Sigma)} \) where \( v^\sigma : \mathcal{V}(\sigma) \to \mathcal{M}(\sigma) \). As usual, given \( x^\sigma \) and \( a \in \mathcal{M}(\sigma) \), we let \( v[a/x^\sigma] \) be the valuation that takes \( x^\sigma \) to \( a \) and which is equal to \( v \) everywhere else. Given a valuation \( v \), each first-order term \( a \in \text{Ter}(\Sigma, \mathcal{V})(\sigma) \) induces an individual \( [a]v \in \mathcal{M}(\sigma) \) in the obvious way.

Definition 6.11. Let \( A \) be a first-order formula over a first-order \( \Sigma \) be a signature.

1. Given a \( \Sigma \)-structure \( \mathcal{M} \) and a valuation \( v \), we say that \( A \) is satisfied in \( \mathcal{M} \) under \( v \) if \( \mathcal{M}, v \models A \), where the relation \( \mathcal{M}, v \models A \) is defined in Fig. 9.

2. Given a \( \Sigma \)-structure \( \mathcal{M} \), we say that \( A \) is satisfiable in \( \mathcal{M} \) if \( \mathcal{M}, v \models A \) for some valuation \( v \).

We say that \( A \) is satisfiable if \( A \) is satisfiable in some \( \Sigma \)-structure \( \mathcal{M} \).

3. Given a \( \Sigma \)-structure \( \mathcal{M} \), we say that \( A \) is valid in \( \mathcal{M} \) (notation \( \mathcal{M} \models A \)) if \( A \) is satisfied in \( \mathcal{M} \) under all valuations \( v \).

We say that \( A \) is valid (notation \( \models A \)) if \( A \) is valid in all \( \Sigma \)-structures \( \mathcal{M} \).

Example 6.12. Assume that \( x^\sigma \) is not free in \( B \). Then the following formulae are valid:

1. \( (\forall \sigma)(A(x^\sigma) \Rightarrow B) \iff ((\exists \sigma)A(x^\sigma) \Rightarrow B) \)
2. \( (\exists \sigma)(A(x^\sigma) \Rightarrow B) \iff ((\forall \sigma)A(x^\sigma) \Rightarrow B) \)
6. First-Order Predicate Logic

\[
\begin{align*}
(Ax) & \quad \frac{}{\Delta \vdash A} (A \in \Delta) \\
(\top-I) & \quad \frac{}{\Delta \vdash \top} \\
(\perp-E) & \quad \frac{}{\Delta \vdash \bot} \quad (\bot-E) \\
(\Rightarrow-I) & \quad \frac{\Delta, A \vdash B}{\Delta \vdash A \Rightarrow B} \\
(\Rightarrow-E) & \quad \frac{\Delta \vdash A \Rightarrow B \quad \Delta \vdash A}{\Delta \vdash B} \\
(\land-I) & \quad \frac{\Delta \vdash A \quad \Delta \vdash B}{\Delta \vdash A \land B} \\
(\land_1-E) & \quad \frac{\Delta \vdash A \land B}{\Delta \vdash A} \\
(\land_2-E) & \quad \frac{\Delta \vdash A \land B}{\Delta \vdash B} \\
(\lor_1-I) & \quad \frac{\Delta \vdash A}{\Delta \vdash A \lor B} \\
(\lor_2-I) & \quad \frac{\Delta \vdash B}{\Delta \vdash A \lor B} \\
(\lor-E) & \quad \frac{\Delta \vdash A \lor B \quad \Delta, A \vdash C \quad \Delta, B \vdash C}{\Delta \vdash C} \\
(\forall-I) & \quad \frac{\Delta \vdash A}{\Delta \vdash (\forall x^\sigma) A} (x^\sigma \notin \text{FV}(\Delta)) \\
(\forall-E) & \quad \frac{\Delta \vdash (\forall x^\sigma) A}{\Delta \vdash A[x^\sigma/x]} \\
(\exists-I) & \quad \frac{\Delta \vdash A[a^\sigma/x^\sigma]}{\Delta \vdash (\exists x^\sigma) A} \\
(\exists-E) & \quad \frac{\Delta \vdash (\exists x^\sigma) A \quad \Delta, A \vdash B}{\Delta \vdash B} (x^\sigma \notin \text{FV}(\Delta, B))
\end{align*}
\]

Figure 10: Natural Deduction Rules for Intuitionistic First-Order Predicate Logic.

6.2. Natural Deduction for First-Order Predicate Logic

Recall from §2.1 (resp. §2.3) the system NJ₀ (resp. NK₀) of natural deduction for intuitionistic (resp. classical) propositional logic. Natural deduction for intuitionistic (resp. classical) first-order predicate logic is given by extending NJ₀ (resp. NK₀) with rules for universal (\(\forall\)) and existential (\(\exists\)) quantifiers.

Formally, fix a first-order signature \(\Sigma\) and a set \(V\) of \(\Sigma\)-sorted first-order variables. Natural deduction for intuitionistic first-order predicate logic (NJ₁) over \((\Sigma, V)\) is given by the deduction rules for Fig. 1, where given \(\Delta = A_1, \ldots, A_n\), we write \(\text{FV}(\Delta)\) for \(\text{FV}(A_1) \cup \cdots \cup \text{FV}(A_n)\). Natural deduction for classical first-order predicate logic (NK₁) over \((\Sigma, V)\) is NJ₁ augmented with the excluded middle (EM) (Def. 2.19, §2.2.1).

Remark 6.13. Similarly as in §2.1 (Rem. 2.8) we shall informally speak of intuitionistic and classical predicate logics for the deduction systems NJ₁ and NK₁. We again insist on the fact that there are different possible deduction systems for these logics.

The remaining of this §6.2 is organized as follows. We state in §6.2.1 the expected usual easy structural properties of NJ₁ and NK₁. The main results relating syntax and semantics of (classical) first-order logic are surveyed in §6.2.2. In §6.2.3 we briefly indicate the extensions to first-order logic of the negative translations from §2.5. The undecidability of provability in NJ₁ and NK₁ is proven in §6.2.4, using material from §3.4.1 and §3.7 on the untyped \(\lambda\)-calculus and Combinatory Logic. The failure of the extension
In Intuitionistic First-Order Predicate Logic (NJ$_1$):
\[
\vdash (\exists x^\sigma)A(x^\sigma) \Rightarrow B \iff (\forall x^\sigma)(A(x^\sigma) \Rightarrow B)
\]
\[
\vdash \neg(\exists x^\sigma)A(x^\sigma) \iff (\forall x^\sigma)\neg A(x^\sigma)
\]
\[
\vdash \neg\neg(\exists x^\sigma)A(x^\sigma) \iff (\forall x^\sigma)\neg\neg A(x^\sigma)
\]

In Classical First-Order Predicate Logic (NK$_1$):
\[
\vdash (\exists x^\sigma)(A(x^\sigma) \Rightarrow B) \iff (\forall x^\sigma)A(x^\sigma) \Rightarrow B
\]

Table 3: Some Laws of First-Order Predicate Logic, where $x^\sigma \notin \text{FV}(B)$.

of Glivenko’s Theorem 2.48 (§2.6) to the full language of first-order logic is discussed in §6.2.5.

Last but not least, the distinctive properties of NJ$_1$ over NK$_1$, namely the Disjunction Property and the analogous **Witness Property** for existential quantifications, are stated in §6.2.6, proved in §6.3.3 and further discussed in §6.4.6.

But before, let us look at some examples!

**Example 6.14.** In NJ$_1$ we have \( \vdash (\forall x^\sigma)A \Rightarrow (\exists x^\sigma)A \) with the proof tree
\[
\begin{array}{c}
(\forall x^\sigma)A \vdash (\exists x^\sigma)A \\
(\forall x^\sigma)A \vdash A \\
(\forall x^\sigma)A \vdash (\exists x^\sigma)A
\end{array}
\]

**Exercise 6.15.** Show that the following, where $x^\sigma \notin \text{FV}(B)$, are derivable in NJ$_1$:
(1) \( \vdash (\forall x^\sigma)(A(x^\sigma) \Rightarrow B) \Rightarrow ((\exists x^\sigma)A(x^\sigma) \Rightarrow B) \)
(2) \( \vdash ((\exists x^\sigma)A(x^\sigma) \Rightarrow B) \Rightarrow (\forall x^\sigma)(A(x^\sigma) \Rightarrow B) \)
(3) \( \vdash (\exists x^\sigma)(A(x^\sigma) \Rightarrow B) \Rightarrow ((\forall x^\sigma)A(x^\sigma) \Rightarrow B) \)

**Exercise 6.16.** Assume that $x^\sigma$ is not free in $B$. Show that in NJ$_1$ we have
\[
\vdash (\forall x^\sigma)(\neg A(x^\sigma) \Rightarrow B) \Rightarrow \neg(\exists x^\sigma)(\neg A(x^\sigma) \Rightarrow B)
\]

**Example 6.17.** Combining Ex. 6.15 and Ex. 6.16, we obtain the laws summarized in Table 3. In particular, NK$_1$ proves the following well-known **Drinker’s Paradox**:
\[
\vdash (\exists x^\sigma)(A(x^\sigma) \Rightarrow (\forall x^\sigma)A(x^\sigma))
\]

Table 4 displays some further usual laws (see e.g. [vD04, Lem. 5.2.1]).

**Exercise 6.18.** Show that in NJ$_1$ we have \( \vdash \neg(\forall x^\sigma)A(x^\sigma) \Rightarrow (\forall x^\sigma)\neg A(x^\sigma) \)
6. First-Order Predicate Logic

In Intuitionistic First-Order Predicate Logic ($\mathcal{NJ}_1$):

$\vdash (\exists x^\sigma)(A(x^\sigma) \lor B(x^\sigma)) \iff ((\exists x^\sigma)A(x^\sigma) \lor (\exists x^\sigma)B(x^\sigma))$

$\vdash (\exists x^\sigma)(A(x^\sigma) \land C) \iff ((\exists x^\sigma)A(x^\sigma) \land C)$

$\vdash (\exists x^\sigma)(C \Rightarrow A(x^\sigma)) \Rightarrow (C \Rightarrow (\exists x^\sigma)A(x^\sigma))$

$\vdash (\forall x^\sigma)(C \Rightarrow A(x^\sigma)) \iff (C \Rightarrow (\forall x^\sigma)A(x^\sigma))$

$\vdash (\forall x^\sigma)A(x^\sigma) \land (\forall x^\sigma)B(x^\sigma) \iff (\forall x^\sigma)(A(x^\sigma) \land B(x^\sigma))$

$\vdash (\forall x^\sigma)A(x^\sigma) \lor C \Rightarrow (\forall x^\sigma)(A(x^\sigma) \lor C)$

In Classical First-Order Predicate Logic ($\mathcal{NK}_1$):

$\vdash (\exists x^\sigma)(C \Rightarrow A(x^\sigma)) \iff (C \Rightarrow (\exists x^\sigma)A(x^\sigma))$

$\vdash (\forall x^\sigma)(C \lor A(x^\sigma)) \iff (C \lor (\forall x^\sigma)A(x^\sigma))$

Table 4: Further Laws of First-Order Predicate Logic, where $x^\sigma \notin \text{FV}(C)$.

6.2.1. Structural Properties

Similarly as for $\mathcal{NJ}_0$, the following basic properties are proved by induction on derivations.

**Lemma 6.19** (Structural Rules). The following properties hold in $\mathcal{NJ}_1$ and $\mathcal{NK}_1$:

- **(weakening)** if $\Delta \vdash A$ then $\Delta, B \vdash A$;
- **(contraction)** if $\Delta, B, B \vdash A$ then $\Delta, B \vdash A$;
- **(exchange)** if $\Delta, B, \Delta', C, \Delta'' \vdash A$ then $\Delta, C, \Delta', B, \Delta'' \vdash A$.

We shall also make use of the following usual fact on stability of provability under substitution of first-order terms.

**Lemma 6.20** (Substitution). In $\mathcal{NJ}_1$ and $\mathcal{NK}_1$, if $\Delta \vdash A$ then $\Delta[a^\sigma/x^\sigma] \vdash A[a^\sigma/x^\sigma]$.

6.2.2. Soundness and Completeness w.r.t. the Classical Semantics: Theories

Deduction in $\mathcal{NK}_1$ (and thus in $\mathcal{NJ}_1$) is sound w.r.t. the semantics of §6.1.3. Say that a sequent $A_1, \ldots, A_n \vdash A$ is **valid** if the formula $(A_1 \times \cdots \times A_n) \Rightarrow A$ is valid in the sense of Def. 6.11.

**Proposition 6.21.** If $\Delta \vdash A$ is derivable in $\mathcal{NK}_1$, then $\Delta \vdash A$ is valid.

Proposition 6.21 fails without the side conditions in the rules ($\forall$-I) and ($\exists$-E) of Fig. 1.
6. First-Order Predicate Logic

Example 6.22. Replacing either of the rules \((\forall\text{-I})\) and \((\exists\text{-E})\) with
\[
\Delta \vdash A \quad \text{or} \quad \Delta \vdash (\exists x^\sigma)A \quad \Delta, A \vdash B
\]
would result in unsound systems, since in each case we have \((\exists x^\sigma)A(x^\sigma) \vdash (\forall x^\sigma)A(x^\sigma)\).
Indeed, the wrong \(\forall\)-rule gives
\[
(\exists x^\sigma)A(x^\sigma) \vdash (\exists x^\sigma)A(x^\sigma) \quad (\exists x^\sigma)A(x^\sigma), A(x^\sigma) \vdash A(x^\sigma)
\]
where the instance of \((\exists\text{-E})\) respects the side condition \(x^\sigma \notin \text{FV}\((\exists x^\sigma)A(x^\sigma), (\forall x^\sigma)A(x^\sigma)\)\), while the wrong \(\exists\text{-rule gives}\)
\[
(\exists x^\sigma)A(x^\sigma) \vdash (\exists x^\sigma)A(x^\sigma) \quad (\exists x^\sigma)A(x^\sigma), A(x^\sigma) \vdash A(x^\sigma)
\]
where the instance of \((\forall\text{-I})\) respects the side condition \(x^\sigma \notin \text{FV}\((\exists x^\sigma)A(x^\sigma), (\forall x^\sigma)A(x^\sigma)\)\).

Similarly as with propositional logic, intuitionistic predicate logic is not complete w.r.t. the classical semantics. But it is indeed complete w.r.t. weaker semantics, see [SU06, §8.5] (see also [vD04, §5.3]).
On the other hand, classical predicate logic is complete w.r.t. the classical semantics. We recall here the relevant statements.

Definition 6.23. Let \(\Phi\) be an arbitrary set of sentences and let \(A\) be a sentence.

1. We say that \(\Phi\) is \textbf{valid} in \(M\) (or that \(M\) is a \textbf{model} of \(\Phi\)), notation \(M \models \Phi\), if \(M \models A\) for each \(A \in \Phi\).

2. We write \(\Phi \models A\) if \(M \models A\) whenever \(M \models \Phi\).

3. We write \(\Phi \vdash_{NK_1} A\) if there is a finite list \(\Delta \subseteq \Phi\) (i.e. \(A \in \Phi\) for each \(A \in \Delta\)) such that \(\Delta \vdash A\) is derivable in \(NK_1\).

Note that \(\Phi \vdash A\) trivially implies \(\Phi \models A\).

Theorem 6.24 (Completeness [vD04, Thm. 3.1.3]). If \(\Phi \models A\) then \(\Phi \vdash_{NK_1} A\).

Corollary 6.25 (Compactness). Fix a set of sentences \(\Phi\). If for every finite \(\Phi_0 \subseteq \Phi\) there is a model \(M\) such that \(M \models \Phi_0\), then there is a model \(M\) such that \(M \models \Phi\).

\textbf{Proof.} Exercise! \(\square\)

We conclude with the notion of theory, which shall be of future use. Intuitively, a classical (resp. intuitionistic) theory is a set of sentences which is closed under classical (resp. intuitionistic) deduction.

74
6. First-Order Predicate Logic

Definition 6.26 (Theory). Let $\Phi$ be a set of sentences.

1. We say that $\Phi$ is a **classical** theory if $A \in \Phi$ whenever $\Phi \vdash_{NK_1} A$.

2. We say that $\Phi$ is an **intuitionistic** theory if $A \in \Phi$ whenever $\Phi \vdash_{NJ_1} A$, where $\Phi \vdash_{NJ_1} A$ if there is a finite list $\Delta \subseteq \Phi$ such that $\Delta \vdash A$ in $NJ_1$.

A theory $\Phi$ is **consistent** if $\Phi \not\vdash_{ND} \bot$ (where $ND$ is $NK_1$ for a classical theory and $ND$ is $NJ_1$ for an intuitionistic one).

In both cases (classical or intuitionistic), every set of sentences $\Phi$ is contained in a least (classical or intuitionistic) theory $\text{th}(\Phi)$. Note that the Completeness Theorem 6.24 can be rephrased as:

- Every consistent classical theory has a model.

6.2.3. Negative Translations

The negative translations discussed in §2.5 extend to first-order predicate logic.

Definition 6.27 (Negative Translation). Extending Def. 2.37, the formula $A^\neg$ is defined by induction on $A$ as follows:

$$
P(a_1^{\sigma_1}, \ldots, a_n^{\sigma_n})^\neg := \neg \neg P(a_1^{\sigma_1}, \ldots, a_n^{\sigma_n})$$

$$\top^\neg := \top$$

$$\bot^\neg := \bot$$

$$(A \Rightarrow B)^\neg := A^\neg \Rightarrow B^\neg$$

$$(A \land B)^\neg := A^\neg \land B^\neg$$

$$(A \lor B)^\neg := \neg \neg (A^\neg \lor B^\neg)$$

$$((\forall x^\sigma)A)^\neg := (\forall x^\sigma)A^\neg$$

$$((\exists x^\sigma)A)^\neg := \neg \neg (\exists x^\sigma)A^\neg$$

The following are the respective extensions of Lem. 2.38 and Thm. 2.39.

Lemma 6.28. For each formula $A$, $NJ_1$ proves $\neg \neg A^\neg \vdash A^\neg$.

Theorem 6.29. If $A_1, \ldots, A_n \vdash A$ is derivable in $NK_1$, then $A_1^\neg, \ldots, A_n^\neg \vdash A^\neg$ is derivable in $NJ_1$.

We shall discuss Lem. 6.28 and Thm. 6.29 as (almost) direct instances of Prop. 7.67 in §7.3.4 below (on Friedman’s Translation of classical to intuitionistic first-order arithmetic).

Corollary 6.30. If $\vdash A$ is derivable in $NK_1$, then $\vdash A^\neg$ is derivable in $NJ_1$.

Remark 6.31 (On Minimal Logic). Remark 2.41 extends to intuitionistic first-order logic, in the sense that if $\vdash A$ in $NK_1$ then $\vdash A^\neg$ can be derived in $NJ_1$ without (ExFalso). It again suffices to observe that the statement of Lem. 6.28 actually holds in minimal logic and that $\bot \vdash A^\neg$ is provable in minimal logic for each formula $A$. We again refer to [TvD88a, Chap. 2, §3] for details.
6. First-Order Predicate Logic

\[(\forall x) (x = sk_{\beta_0} x) \quad (\forall x, y) (x = sk_{\beta_0} y \Rightarrow y = sk_{\beta_0} x)\]

\[(\forall x, y, z) (x = sk_{\beta_0} y \Rightarrow y = sk_{\beta_0} z \Rightarrow x = sk_{\beta_0} z)\]

\[(\forall x', y', y') (x = sk_{\beta_0} x' \Rightarrow y = sk_{\beta_0} y' \Rightarrow y y = sk_{\beta_0} x' y')\]

\[(\forall x, y) (x y = sk_{\beta_0} x) \quad (\forall x, y, z) (s x y z = sk_{\beta_0} x z (y z))\]

Figure 11: Closed Formulae for \(\Gamma_0\).

Remark 6.32 (On the G"odel-Gentzen and Kolmogorov Translations). Extending Rem. 2.43, the original G"odel-Gentzen translation (see e.g. [TvD88a, Chap. 2, Def. 3.4] or [vD04, Def. 5.2.7]) assumes

\[\neg (\forall x) \neg A \neg \neg \neg \]

The Kolmogorov translation \((-)\neg\neg\) (see e.g. [TvD88a, Chap. 2, 3.7]) extends with

\[P(a_1^{\sigma_1}, \ldots, a_n^{\sigma_n})\neg\neg := \neg\neg P(a_1^{\sigma_1}, \ldots, a_n^{\sigma_n})\]

6.2.4. Undecidability

A fundamental fact on (classical) first-order logic is the undecidability of provability (or equivalently of validity, by the Completeness Theorem 6.24, §6.2.2). This result, known as Church’s Theorem, can be proved in many ways. See e.g. [BBJ07, §11] or [vD04, Cor. 7.7.12]. Note that Cor. 6.30 (§6.2.3) reduces the undecidability of provability in \(NJ_1\) to the undecidability of provability in \(NK_1\) ([SU06, Cor. 8.3.2]). We note here that having at hand the (pure) untyped \(\lambda\)-calculus (actually Combinatory Logic, §3.7) allows for a quite direct proof of undecidability of \(NJ_1\) and \(NK_1\). See [Bar84, 7.4.11] for references on the following argument.

We consider the (one-sorted) finite first-order signature \(\Sigma(C_0)\) whose closed terms are the closed terms \(t \in C_0\) of combinatory logic (§3.7), i.e. the terms over the grammar:

\[t, u \in C_0 := t \mid u \mid s \mid k\]

Remark 6.33. Note that \(\Sigma(C_0)\) actually has a binary function symbol for application (similarly as in §3.2.1).

We also assume that \(\Sigma(C_0)\) has one (infix) binary predicate symbol \((-) = sk_{\beta_0} (-)\). Let \(\Gamma_0\) be the (finite) set of (closed) formulae consisting of the axioms of Fig. 3 (§3.7.1) together with the formulae of Fig. 11.

Proposition 6.34. The following are equivalent for \(t, u \in C_0\):

(i) \(t = sk_{\beta_0} u\) (in the sense of §3.7.1);
(ii) $\Gamma_0 \vdash t =_{sk_0} u$ in $NJ_1$;

(iii) $\Gamma_0 \vdash t =_{sk_0} u$ in $NK_1$.

**Proof.** Exercise! \(\square\)

Since the set $\Gamma_0$ is finite and since $=_{sk_0}$ is undecidable (Cor. 3.65, § 3.7.1), Prop. 6.34 gives the following.

**Theorem 6.35** (Church). The following problems are undecidable:

- Given a finite first-order signature $\Sigma$ and a first-order formula $A$ over $\Sigma$, decide whether $\vdash A$ in $NJ_1$.
- Given a finite first-order signature $\Sigma$ and a first-order formula $A$ over $\Sigma$, decide whether $\vdash A$ in $NK_1$.

Note that the above argument for Thm. 6.35 also gives the undecidability of the $(\forall, \Rightarrow)$-fragment of (minimal) first-order logic. See also [SU06, § 8.8] for a proof of undecidability of $NJ_1$ (actually also of its $(\forall, \Rightarrow)$-fragment) relying on the normalization of proof-terms (§ 6.3).

### 6.2.5. The Failure of Glivenko’s Theorem for Full First-Order Logic

As noted in Table 3, $NJ_1$ proves

$$\vdash (\exists x^\sigma)\neg\neg A(x^\sigma) \Rightarrow \neg\neg(\exists x^\sigma)A(x^\sigma)$$

Recalling the proof of Prop. 2.47 (§2.6), it is easy to see that Glivenko’s Theorem 2.48 extends to the following.

**Theorem 6.36.** Let $A$ be a first-order formula with no universal quantifier $(\forall x^\sigma)$. Then $NK_1$ proves $\vdash A$ if and only if $NJ_1$ proves $\vdash \neg\neg A$.

However, Thm. 6.36 does not extend to the full language of first-order logic. In particular:

**Proposition 6.37.** $NJ_1$ proves neither of the following:

1. $\vdash \neg(\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n}) (P(x_1^{\sigma_1} \ldots x_n^{\sigma_n}) \lor \neg P(x_1^{\sigma_1} \ldots x_n^{\sigma_n}))$
2. $\vdash (\forall x^\sigma)\neg\neg A \Rightarrow \neg\neg(\forall x^\sigma)A$

Proposition 6.37 has easy semantic proofs (outside the scope of this course), see [SU06, Prop. 8.5.3] (also [vD04, 5.3(f), p. 170] or [TvD88a, Ex. 5.9, Chap. 2]). Note that Prop. 6.37.(2) follows from Prop. 6.37.(1).

**Remark 6.38.** The formula of Prop. 6.37.(2) is called the **Double Negation Shift** (DNS). It plays a crucial role in semi-constructive extensions of intuitionistic arithmetic, in relation to arithmetic formulations of weak versions of the Axiom of Choice (see e.g. [BBC98, BO05], also [Koh08, §11], outside the scope of this course).
6. First-Order Predicate Logic

Remark 6.39. We shall see in §7.3.3 (actually §8.3) that NJ₁ is compatible with some instances of
\[ (\neg \forall \text{-EM}) \vdash \neg (\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n} (A \lor \neg A)) \]
in the sense that NJ₁ augmented with some instances of (\neg \forall \text{-EM}) is consistent (i.e. does not prove \vdash \bot). This can also be shown with semantic methods ([SU06, Prop. 8.5.3] or e.g. [TvD88a, Ex. 5.9, Chap. 2]), see also [TvD88a, Prop. 3.4, Chap. 4].

6.2.6. Extraction

The distinctive properties of NJ₁ over NK₁ are the following. The proofs are deferred to §6.3.3. A comparison with NK₁ is sketched in §6.4.6.

Theorem 6.40. In intuitionistic first-order predicate logic (NJ₁),

(1) \vdash \bot is not derivable;

(2) from a proof of \vdash A_1 \lor A_2 one can effectively compute an \( i \in \{1, 2\} \) and a proof of \vdash A_i;

(3) \vdash P(x_1, \ldots, x_n) \lor \neg P(x_1, \ldots, x_n) is not derivable (where \( P \in \text{Pred} (\Sigma)(n) \));

(4) from a proof of \vdash (\exists x^\sigma)A one can effectively compute a first-order term \( a^\sigma \) and a proof of \vdash A[a^\sigma/x^\sigma].

Theorem 6.40.(4) is often called the Witness (or Existence) Property. The following consequence of Thm 6.40.(4) is one of the main properties of NJ₁.

Corollary 6.41. From a proof of \vdash (\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n})(\exists y^\tau)A in NJ₁ (where \( n \geq 1 \) and \( A \) has free variables among \( x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}, y^\tau \)), one can effectively compute a first-order term \( a^\tau = a^\tau(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) \) and a proof of \vdash (\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n})A[a^\tau/y^\tau] in NJ₁.

Proof. We omit sorts. From a proof of \vdash (\forall x_1 \ldots x_n)(\exists y)A in NJ₁ one gets a proof of \vdash (\exists y)A. Then Thm. 6.40.(4) provides a first-order term \( a = a(x_1, \ldots, x_n) \) and a proof of \vdash A[a/y] in NJ₁ (note that the variables of \( a \) possibly not in \( A \) can be substituted by variables among \( x_1, \ldots, x_n \)). One thus obtains a proof of \vdash (\forall x_1 \ldots x_n)A[a/y].

The effective character of Thm. 6.40 and Cor. 6.41 should be contrasted with the undecidability of provability in NJ₁ (Thm. 6.35, §6.2.4).

We shall prove Thm. 6.40 with a normalizing \( \lambda \)-calculus of proof-terms in §6.3 below. Corollary 6.41 is [SU06, Cor. 8.3.4 & Cor. 8.3.5], a particular case of [Bus98a, Thm. 3.1.3] (see also [TS00, Thm. 4.2.3 & Thm. 4.2.4]), all obtained by normalization of Gentzen-style sequent calculi. Weaker properties can be obtained by semantic methods (see e.g. [vD04, Thm. 5.4.2 & Thm. 5.4.3]).

We come back on Cor. 6.41 in §6.4.6 below.
6. First-Order Predicate Logic

6.3. Proof-Terms for Intuitionistic First-Order Predicate Logic

We now turn to proof-terms for $NJ_1$. Besides [SU06, §8.7], standard references include [Gal95], [TvD88b, Chap. 10, §8] and [TS00, §2.2].

Consider a first-order signature $\Sigma$. For simplicity we assume that $\Sigma$ is one-sorted, but the following is easily extended to many-sorted signatures. We use the notational conventions of §6.1 for one-sorted signatures.

The proof-terms for $NJ_0$ (§4.4) can be adapted to yield proof-terms for $NJ_1$. The main ideas come from the Brouwer-Heyting-Kolmogorov (BHK) interpretation of intuitionistic first-order predicate logic. Recall from §4.1 that the BHK interpretation is an informal interpretation of intuitionistic proofs. The clauses given in §4.1 for propositional logic may be extended as follows for (intuitionistic) first-order logic:

- a "proof" of $(\forall x)A$ is a "function" which takes a term $a \in \text{Ter}(\Sigma, V)$ to a "proof" of $A[a/x]$;
- a "proof" of $(\exists x)A$ is a (dependent) pair of a term $a \in \text{Ter}(\Sigma, V)$ and a "proof" of $A[a/x]$.

where the term "proof" should be understood as some informal notion of "witness of evidence", and where the term "function" is not fully specified. We refer to [SU06, §8.2] and (again) to [TvD88a, Chap. 1, §3.1] for more on the BHK interpretation of intuitionistic first-order logic.

In view of the Curry-Howard correspondence for $NJ_0$, following Rem. 4.44 (§4.4.5) it makes sense to think that the word "function" above refers to some $\lambda$-abstraction. We shall extend the proof-terms of §4.4 with the following constructs:

- a $\lambda$-abstraction $\lambda x.t$ where $x \in V$ is a first-order variable, and the corresponding elimination $ta$ where $a \in \text{Ter}(\Sigma, V)$ is a first-order term;
- a pairing $\langle a, t \rangle$ where $a \in \text{Ter}(\Sigma, V)$, and the corresponding elimination $\text{let } \langle x, y \rangle = t \text{ in } u$, where $x \in V$ (see Fig. 12).

Formally, the proof-terms for $NJ_1$ over $(\Sigma, V)$ are given by the following grammar:

$$ t, u \in \Lambda(\Sigma, V) ::= x \mid \lambda x.t \mid tu \mid \langle t, u \rangle \mid \pi_1 t \mid \pi_2 t \mid \text{in}_1 t \mid \text{in}_2 t \mid \langle \rangle \mid \text{case}_{\bot} t \{ \} \mid \text{case } t \{ \text{in}_1 x_1 \mapsto u_1 \mid \text{in}_2 x_2 \mapsto u_2 \} \mid \lambda x.t \mid ta \mid \langle a, t \rangle \mid \text{let } \langle x, y \rangle = t \text{ in } u $$

where $a \in \text{Ter}(\Sigma, V)$ and $x \in V$.

Note that we thus have two universes of terms:

- the first-order terms $a, b, \ldots \in \text{Ter}(\Sigma, V)$, with variables $x, y, z, \ldots \in V$;
- the proof-terms $t, u, \ldots \in \Lambda(\Sigma, V)$, with variables $x, y, z, \ldots \in V$ (§3.2.1).
6. First-Order Predicate Logic

\[
\begin{align*}
(\forall\text{-I}) & \quad \mathcal{E} \vdash t : A \quad \mathcal{E} \vdash \lambda x.t : (\forall x)A \\
(\forall\text{-E}) & \quad \mathcal{E} \vdash t : (\forall x)A \\
\end{align*}
\]

Figure 12: Proof-Terms for Intuitionistic First-Order Predicate Logic: Quantifier Rules.

**Warning 6.42** (Variable Binding). The variable \(x\) is bound in \(\lambda x.t\). Moreover, the construction \(\text{let} \ (x,y) = t \text{ in } u\) binds \(x\) and \(y\) in \(u\) (but not in \(t\)). We thus assume the corresponding extension of \(\alpha\)-conversion (§3.2.3 and §3.2.4).

The notions of free-variable (Def. 3.3, §3.2.3) are adapted accordingly.

Concerning typing, we take as types the formulae of first-order predicate logic over \((\Sigma, V)\), namely:

\[
A, B ::= \text{P}(a_1, \ldots, a_n) \mid A \Rightarrow B \mid A \land B \mid A \lor B \mid \top \mid \bot
\]

where \(\text{P} \in \text{Pred}(\Sigma)(n)\) and \(a_i \in \text{Ter}(\Sigma, V)\) for each \(i = 1, \ldots, n\).

The typing rules are those of §4.4.5 augmented with the additional typing rules of Fig. 12, where given \(\mathcal{E} = x_1 : A_1, \ldots, x_n : A_n\), we let \(\text{FV}(\mathcal{E})\) stand for \(\text{FV}(A_1) \cup \cdots \cup \text{FV}(A_n)\) (not to be confused with \(\text{dom}(\mathcal{E}) = \{x_1, \ldots, x_n\}\)).

Theorem 4.37 (§4.4.5) trivially extends, with the erasure of proof-terms from typing rules depicted in Fig. 13.

**Theorem 6.43.** The sequent \(A_1, \ldots, A_n \vdash A\) is derivable in \(\text{NJ}_1\) if and only if there is a proof-term \(t\) such that \(x_1 : A_1, \ldots, x_n : A_n \vdash t : A\).

The other important properties of \(\text{NJ}_1\) (essentially consequences of Thm. 6.43 together with suitable normalization results) are presented in §6.3.3 and further discussed in §6.4.6.

**Example 6.44.** For instance \(\vdash \lambda h.(y, hy) : (\forall x)A \Rightarrow (\exists x)A\) with typing derivation

\[
\begin{align*}
\rule{0pt}{2ex} & \quad \vdash h : (\forall x)A \vdash h : (\forall x)A \\
\rule{0pt}{2ex} & \quad \vdash h : (\forall x)A \vdash hy : A[y/x] \\
\rule{0pt}{2ex} & \quad \vdash h : (\forall x)A \vdash (y, hy) : (\exists x)A \\
\rule{0pt}{2ex} & \quad \vdash \lambda h.(y, hy) : (\forall x)A \Rightarrow (\exists x)A
\end{align*}
\]

**Exercise 6.45.** Give a proof term \(t\) such that \(\vdash t : \neg(\forall x)A(x) \Rightarrow (\forall x)\neg A(x)\).

**Remark 6.46** (Open Terms and Assumption-Free Proofs). Recall the proof-term \(\vdash \lambda h.(y, hy) : (\forall x)A \Rightarrow (\exists x)A\) from Ex. 6.44. Note that \(\lambda h.(y, hy)\) is open (it contains \(y\) free), while the formulae \((\forall x)A\) and \((\exists x)A\) may be closed. If \(\text{Ter}(\Sigma, V)\) contains some
closed term (i.e. if \( \Sigma \) has at least one constant), then we might replace \( y \) with such a closed term, and obtain a closed proof-term for \( (\forall x)A \Rightarrow (\exists x)A \).

However \( (\forall x)A \Rightarrow (\exists x)A \) is provable and thus valid without any such assumption on \( \Sigma \). This reflects the fact that models of first-order logic are always assumed to be non-empty (see Def. 6.8, §6.1.3).

**Remark 6.47** (On the Side Condition of (\( \exists \)-E)). Note that in the rule

\[
(\exists \text{-E}) \quad \mathcal{E}, y : A \vdash u : B \\
\mathcal{E} \vdash \text{let} \ (x, y) = t \ 	ext{in} \ u : B
\]

the variable \( x \) is required not to occur free in \( \mathcal{E} \) nor \( B \), but it may occur free in the proof-term \( u \). For instance, the proof-term for the \( \text{NJ}_1 \)-derivation

\[
(\exists \text{-E}) \quad (\exists x)A, A \vdash A \\
(\exists x)A, A \vdash (\exists x)A \\
(\exists x)A \vdash (\exists x)A \quad (x \notin \text{FV}((\exists x)A))
\]

is

\[
(\exists \text{-E}) \quad h : (\exists x)A, y : A \vdash y : A \\
h : (\exists x)A \vdash \text{let} \ (x, y) = h \ 	ext{in} \ (x, y) : (\exists x)A \\
(\exists \text{-E}) \quad h : (\exists x)A, y : A \vdash (\exists x)A \\
h : (\exists x)A \vdash \text{let} \ (x, y) = h \ 	ext{in} \ (x, y) : (\exists x)A \\
(\exists \text{-E}) \quad h : (\exists x)A \vdash h : (\exists x)A \\
h : (\exists x)A \vdash (\exists x)A \\
(\exists \text{-E}) \quad (x \notin \text{FV}((\exists x)A))
\]

**Remark 6.48.** The major difference with the case of propositional logic is that first-order terms and variables are incorporated into the world of proof-terms. But first-order terms and proof-terms are still distinct entities. For instance, first-order variables are not declared in typing contexts, which leads to the apparent “paradox” of Rem. 6.46.
This one of the reasons why we refrain from speaking of “Curry-Howard correspondence” here. The second reason is that the λ-terms considered here have no other raison d’être than being proof-terms for NJ₁.

The formalism which is often considered to be more interesting for a Curry-Howard perspective on predicate logic is the setting of dependent types. See [SU06, Chap. 13] or [Uni13, §1] (see also [Bar92, §5.4] for the representation of predicate logic with dependent types). In particular, with dependent types all variables are declared in typing contexts, and there are first-order signatures such that (the analogue of) $(\forall x)A \Rightarrow (\exists x)A$ is the type of no proof-term in the empty context.

### 6.3.1. Structural Properties

We state some basic structural properties on proof-terms, proved by straightforward induction on typing derivations.

**Lemma 6.49** (Structural Properties).

(Weakening) If $\mathcal{E} \vdash t : A$ and $x \notin \text{dom}(\mathcal{E})$ then $\mathcal{E}, x : B \vdash t : A$.

(Contraction) If $\mathcal{E}, x : B, y : B \vdash t : A$ then $\mathcal{E}, x : B \vdash t[y/x] : A$.

(Exchange) If $\mathcal{E}, x : B, \mathcal{E}', y : C, \mathcal{E}'' \vdash t : A$, then $\mathcal{E}, y : C, \mathcal{E}', x : B, \mathcal{E}'' \vdash t : A$.

There are two relevant substitution properties on proof-terms.

**Lemma 6.50** (Substitution for Proof-Terms).

(1) If $\mathcal{E}, y : B \vdash t : A$ and $\mathcal{E} \vdash u : B$, then $\mathcal{E} \vdash t[u/y] : B$.

(2) If $\mathcal{E} \vdash t : A$ then $\mathcal{E}[a/x] \vdash t : A[a/x]$.

### 6.3.2. Beta-Reduction

We now discuss the extension of β-reduction to the proof-terms for NJ₁. Similarly as in §4.4, we shall derive reductions on λ-terms from expected syntactic transformations of proofs.

**Universal Quantifications.** Consider the following reduction of a $(\forall\text{-I})/(\forall\text{-E})$-redex in natural deduction

\[
\frac{\Delta \vdash A}{\Delta \vdash (\forall x)A} \quad (x \notin \text{FV}(\Delta))
\]

\[\vdash \]

\[
\frac{\Delta \vdash A[a/x]}{\Delta \vdash A[a/x]}\]
where $\Pi[a/x]$ is obtained from the Substitution Lemma 6.20 (§6.2), since $x \notin \text{FV}(\Delta)$. This suggests to allow for the following $\beta$-reduction on proof-terms

\[
\dfrac{
\vdash t : A
}{\vdash \lambda x.t : (\forall x)A}
\]

\[
\vdash (\lambda x.t) a : A[a/x]
\]

where $\Pi[a/x]$ is obtained from the Substitution Lemma 6.20 (§6.2), since $x \notin \text{FV}(\Delta)$. This suggests to allow for the following $\beta$-reduction on proof-terms.

We shall just extend $\beta$-reduction on untyped $\lambda$-terms with

\[
(\lambda x.t) a \beta t[a/x]
\]

Existential Quantifications. Consider now the case of a $(\exists$-I)/(\exists$-E$) redex in natural deduction:

\[
\dfrac{
\vdash t : A
}{\vdash \exists x.t : (\exists x)A}
\]

\[
\vdash (\exists x)A \land B
\]

The derivation $\Pi_2[a/x][\Pi_1/A[a/x]]$ is obtained as follows. First, by the Substitution Lemma 6.20 (§6.2), since $x \notin \text{FV}(\Delta, B)$ we have a derivation

\[
\vdash \Delta, A[a/x] \vdash B
\]

Then, $\Pi_2[a/x][\Pi_1/A[a/x]]$ is obtained (similarly as in §4.3.1) by replacing in $\Pi_2[a/x]$ each (Ax) rule

\[
\vdash \Delta' \vdash A[a/x]
\]

(where $\Delta$ is necessarily a prefix of $\Delta'$) by a derivation of $\Delta' \vdash A[a/x]$ obtained from $\Pi_1$ by weakenings (Lem. 6.49, §6.3.1).

This suggests to allow for the following $\beta$-reduction on proof-terms

\[
\dfrac{
\vdash t : A[a/x]
}{\vdash (\lambda x.t)u : B}
\]

\[
\vdash (\exists x)A \land B
\]

where $x \notin \text{FV}(\varepsilon) \cup \text{FV}(B)$. The typing derivation $\Pi_2[a/x][\Pi_1/A[a/x]]$ is obtained similarly as for the case of natural deduction (without proof terms) just described. First, since $x \notin \text{FV}(\varepsilon) \cup \text{FV}(B)$ the Substitution Lemma 6.50.(2) on proof-terms gives a typing derivation
6. First-Order Predicate Logic

**Basic Rules:** extension of \( \triangleright_0 \) (Fig. 5) with

\[
(\lambda x.t) a \Rightarrow t[a/x] \quad \text{let } (x,y) = (a,t) \text{ in } u \Rightarrow u[a/x][t/y]
\]

**Congruence Rules:** \( \triangleright_\beta \) is the least relation containing \( \triangleright_0 \) and closed under the rules of Fig. 5 and

\[
\begin{align*}
t & \Rightarrow t' \quad \text{let } (x,y) = t \text{ in } u & \Rightarrow t\text{ in } u' \\
\lambda x.t & \Rightarrow_\beta \lambda x.t' & \text{let } (x,y) = t \Rightarrow t\text{ in } u \\
\langle a,t \rangle & \Rightarrow_\beta \langle a,t' \rangle & \text{let } (x,y) = t \Rightarrow t\text{ in } u \\
\end{align*}
\]

Figure 14: Extension of Fig. 5 (§4.4.3) for \( \beta \)-Reduction.

\[
\Pi_2[a/x] \\
\frac{}{\mathcal{E}, y : A[a/x] \vdash u[a/y] : B}
\]

We then conclude with Lem. 6.50.(1):

\[
\Pi_2[a/x][\Pi_1/A[a/x]] \\
\frac{}{\mathcal{E} \vdash u[a/x][t/y] : B}
\]

We shall therefore extend \( \beta \)-reduction on untyped \( \lambda \)-terms with

\[
\text{let } (x,y) = (a,t) \text{ in } u \Rightarrow_\beta u[a/x][t/y]
\]

6.3.3. The Full System and its Main Properties

Summarizing the discussion of §6.3.2, we consider on the proof-terms of \( \text{NJ}_1 \) the relation of \( \beta \)-reduction given by extending Fig. 5 (§4.4.3) with Fig. 14. More precisely, we first define the relation \( \triangleright_0 \) with the basic rules of Fig. 14 (and Fig. 5), and then let \( \triangleright_\beta \) be the closure of \( \triangleright_0 \) under the congruence rules of Fig. 14 (and Fig. 5).

The main properties on (typed) \( \beta \)-reduction of §4.4.4 straightforwardly extend to the proof-terms of \( \text{NJ}_1 \).

**Proposition 6.51** (Subject Reduction). If \( \mathcal{E} \vdash t : T \) and \( t \Rightarrow_\beta u \) then \( \mathcal{E} \vdash u : T \).

**Theorem 6.52** (Strong Normalization). If \( \mathcal{E} \vdash t : T \) then \( t \) is strongly \( \beta \)-normalizing.
Theorem 6.52 is proven in §6.5 (Cor. 6.71), by reduction to the strong normalization of the simply-typed λ-calculus with sums and products (Thm. 4.31, §4.4.4, a.k.a. Thm. 5.32, §5.5.3).

**Theorem 6.53** (Confluence). For each typing context E and each type T, the relation $\triangleright_{\beta}$ is confluent on $|E \vdash T|$ (where $|E \vdash T|$ is defined as in Rem. 4.11, §4.2.2).

**Lemma 6.54** (Normal Forms in the Empty Context). Let t be a (possibly open) proof-term typable in the empty context and in $\beta$-normal form. Then t is of one of the following forms:

\[
\lambda x. u \langle \rangle \quad \langle u, v \rangle \quad \text{in}_1 u \quad \text{in}_2 u \quad \lambda x. u \quad \langle a, u \rangle
\]

**Proof.** Exercise!

We now arrive at the main property of NJ$_1$, namely Thm. 6.40 (§6.2.6). Theorem 6.40 is actually an immediate consequence of the following.

**Theorem 6.55.** In intuitionistic first-order predicate logic (NJ$_1$),

1. there is no proof-term t such that $\vdash t : \bot$;
2. if $\vdash t : A_1 \lor A_2$ then there is an $i \in \{1, 2\}$ and a proof-term $u_i$ such that $t \triangleright^* \text{in}_i u_i$ and $\vdash u_i : A_i$;
3. there is no proof-term t such that $\vdash t : P(x_1, \ldots, x_n) \lor \neg P(x_1, \ldots, x_n)$ (where $P \in \text{Pred}(\Sigma)(n)$);
4. if $\vdash t : (\exists x)A$ then there is some first-order term a and some proof-term u such that $t \triangleright^* \langle a, u \rangle$ and $\vdash u : A[a/x]$.

**Proof.** Exercise!

**Remark 6.56.** Let us look at the shape of the proof-terms for Cor. 6.41 (§6.2.6).

Let t such that $\vdash t : (\forall x_1 \ldots x_n)(\exists y)A$. By the results above, we can assume that t is of the form $\lambda x_1 \ldots x_n.u$ with u in $\beta$-normal form. Moreover, since the $x_i$’s are first-order variables, we must have $\vdash u : (\exists y)A$, so that (since u is normal) u is of the form $\langle a, v \rangle$ with $\vdash v : A[a/x]$. It follows that Cor. 6.41 (§6.2.6) could have been obtained from the following:

- A $\beta$-normal proof-term for $(\forall x_1 \ldots x_n)(\exists y)A$ is of the form $\vdash \lambda x_1 \ldots x_n.a, v : (\forall x_1 \ldots x_n)(\exists y)A$ where $\lambda x_1 \ldots x_n.v : (\forall x_1 \ldots x_n)A[a/y]$.

6.4. First-Order Predicate Logic with Equality

The extension of the above logic with equality holds no surprise. We review the syntax and semantics of predicate logic with equality in §6.4.1–§6.4.5. Finally, in §6.4.6 we come back on the witness property of NJ$_1$ (Cor. 6.41, §6.2.6), and briefly compare it to classical logic.
6. First-Order Predicate Logic

\[
\frac{\Delta \vdash a^\sigma \doteq_\sigma a^\sigma}{(\doteq I)} \quad \quad \quad \frac{\Delta \vdash a^\sigma \doteq_\sigma b^\sigma}{\Delta \vdash A[b^\sigma/x^\sigma]} \quad \quad \quad \frac{\Delta \vdash A[a^\sigma/x^\sigma]}{(\doteq E)}
\]

Figure 15: Equality Rules.

6.4.1. The Language of First-Order Predicate Logic with Equality

Let \( \Sigma \) be a first-order signature and \( V \) be a collection of \( \Sigma \)-sorted first-order variables. First-order predicate logic with equality over \((\Sigma, V)\) simply extends first-order predicate logic over \((\Sigma, V)\) with one (binary) sorted atomic equality predicate \((\doteq)\) for each sort \( \sigma \in \text{Sort}(\Sigma) \). Formally, the formulae of first-order predicate logic with equality over \((\Sigma, V)\) are given by the grammar:

\[
A, B ::= (a^\sigma \doteq_\sigma b^\sigma) \mid P(a_1, \ldots, a_n) \\
\quad \mid A \Rightarrow B \mid A \land B \mid A \lor B \mid \top \mid \bot \\
\quad \mid (\forall x^\tau)A \mid (\exists x^\tau)A
\]

where \( a^\sigma, b^\sigma \in \text{Ter}(\Sigma, V)(\sigma) \) and \( P \in \text{Pred}(\Sigma)(\tau_1, \ldots, \tau_n) \) with \( a_i \in \text{Ter}(\Sigma, V)(\tau_i) \) for each \( i = 1, \ldots, n \).

Notation 6.57. In the one-sorted case, we write \((\doteq)\) for the (unique) equality predicate.

Remark 6.58. Similarly as [vD04, §2.6], we have defined first-order logic with equality over arbitrary signatures \( \Sigma \), but we could as well (similarly as [Bus98a, §2]) have defined a notion of signature with equality (i.e. a signature \( \Sigma \) such that each \( \text{Pred}(\Sigma)(\sigma, \sigma) \) contains a distinguished predicate symbol \((\doteq)\)), and speak of logic with equality only when considering signatures with equality.

Our choice stems from the fact that equality is (in general) assumed to satisfy some specific axioms (§6.4.2), which lead to specific interpretation in models (§6.4.3), as well as specific behaviour under negative translations (§6.4.4) and specific proof terms (§6.4.5).

The other notions of §6.1.2 extend straightforwardly to logic with equality:

\[
\text{FV}(a^\sigma \doteq_\sigma b^\sigma) := \text{FV}(a^\sigma) \cup \text{FV}(b^\sigma) \\
(a^\sigma \doteq_\sigma b^\sigma)[c^\tau/y^\tau] := (a^\sigma[c^\tau/y^\tau] \doteq_\sigma b^\sigma[c^\tau/y^\tau])
\]

6.4.2. Deduction for First-Order Predicate Logic with Equality

Natural deduction for intuitionistic (resp. classical) first-order predicate logic with equality is the extension of natural deduction intuitionistic (resp. classical) first-order predicate logic with the additional equality rules of Fig. 15.

Exercise 6.59. Show that intuitionistic first-order predicate logic with equality proves the following:

(1) \( \Delta \vdash (\forall x^\sigma)(x^\sigma \doteq_\sigma x^\sigma) \)
6. First-Order Predicate Logic

(2) \( \Delta \vdash (\forall \sigma)(\forall \theta)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} x^\sigma) \)

(3) \( \Delta \vdash (\forall \sigma)(\forall \theta)(\forall z^\sigma)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} z^\sigma \Rightarrow x^\sigma \stackrel{\sigma}{=} z^\sigma) \)

It is important to make it clear that the rules of Fig. 15 are equivalent to the usual axioms for equality. We refer to \([vD04, \S 2.10]\) and \([Bus98a, \S 2.2.1]\) for equivalent presentations of the same theories.

**Exercise 6.60.** Show that over \(NJ_1\) and \(NK_1\), the equality rules of Fig. 15 are equivalent to the following equality axioms:

\[
\Delta \vdash (\forall x^\sigma)(x^\sigma \stackrel{\sigma}{=} x^\sigma) \quad \Delta \vdash (\forall x^\sigma, y^\sigma)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} x^\sigma)
\]

\[
\Delta \vdash (\forall x^\sigma, y^\sigma, z^\sigma)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} z^\sigma \Rightarrow x^\sigma \stackrel{\sigma}{=} z^\sigma)
\]

**Remark 6.61.** It is well-known (see e.g. \([vD04, \S 2.10]\)) that the axiomatization of equality of Ex. 6.60 could as well have been presented in the (more refined but) equivalent following form

\[
\Delta \vdash (\forall x^\sigma)(x^\sigma \stackrel{\sigma}{=} x^\sigma) \quad \Delta \vdash (\forall x^\sigma, y^\sigma)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} x^\sigma)
\]

\[
\Delta \vdash (\forall x^\sigma, y^\sigma, z^\sigma)(x^\sigma \stackrel{\sigma}{=} y^\sigma \Rightarrow y^\sigma \stackrel{\sigma}{=} z^\sigma \Rightarrow x^\sigma \stackrel{\sigma}{=} z^\sigma)
\]

\[
f \in \text{Fun}(\Sigma)(\sigma_1, \ldots, \sigma_n; \tau) \quad \frac{\Delta \vdash (\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n})(\forall y_1^{\tau_1} \ldots y_n^{\tau_n})(\bigwedge_{1 \leq i \leq n} x_i^{\sigma_i} \stackrel{\sigma_i}{=} y_i^{\tau_i}) \Rightarrow f(x) \stackrel{\tau}{=} f(y)}{P \in \text{Pred}(\Sigma)(\sigma_1, \ldots, \sigma_n) \quad \frac{\Delta \vdash (\forall x_1^{\sigma_1} \ldots x_n^{\sigma_n})(\forall y_1^{\tau_1} \ldots y_n^{\tau_n})(\bigwedge_{1 \leq i \leq n} x_i^{\sigma_i} \stackrel{\sigma_i}{=} y_i^{\tau_i}) \Rightarrow P(x) \Leftrightarrow P(y)}}
\]

### 6.4.3. Models of First-Order Predicate Logic with Equality

A **model** of first-order predicate logic with equality over a signature \(\Sigma\) is simply a model \(M\) of \(\Sigma\) in the sense of Def. 6.8 (\(\S 6.1.3\)). Satisfaction and validity (Def. 6.11) for formulae with equality assume that the atomic formulae \((-) \stackrel{\sigma}{=} (-)\) are interpreted as plain equality over \(M(\sigma)\). Formally, the relation \(M, v \models A\) (Fig. 9) is extended with the clause

\[
M, v \models (a^\sigma \stackrel{\sigma}{=} b^\sigma) \iff \llbracket a^\sigma \rrbracket v = \llbracket b^\sigma \rrbracket v
\]

Deduction in (intuitionistic and) classical first-order predicate logic with equality is sound w.r.t. the semantics of first-order predicate logic with equality.

Concerning completeness and compactness, (in the case of classical logic) Thm. 6.24 and Cor. 6.25 (\(\S 6.2.2\)) extend to the following, where \(\Phi, A\) consist of sentences with equality.

**Theorem 6.62** (Completeness \([vD04, \text{Thm. } 3.1.3]\)). If \(\Phi \models A\) then \(\Phi \vdash A\).

**Corollary 6.63** (Compactness). Fix a set of sentences \(\Phi\). If for every finite \(\Phi_0 \subseteq \Phi\) there is a model \(M\) such that \(M \models \Phi_0\), then there is a model \(M\) such that \(M \models \Phi\).
6. First-Order Predicate Logic

\[
\frac{(\doteq) -1}{\mathcal{E} \vdash \text{eq}_I \ a : a \doteq a} \quad \frac{(\doteq) -E}{\mathcal{E} \vdash t : a \doteq b \quad \mathcal{E} \vdash u : A[a/x]}{\mathcal{E} \vdash \text{eq}_E \ a \ b \ t \ u : A[b/x]}
\]

Figure 16: Typing Rules for Equality.

\textbf{Remark 6.64.} It is fairly standard to obtain Thm. 6.62 from Thm. 6.24 (completeness of first-order logic without equality, §6.2.2). The trick is the following. Given a first-order signature \( \Sigma \), let \( \Sigma(\doteq) \) be the extension of \( \Sigma \) with one additional predicate symbol \( (\doteq) \) in \( \text{Pred}(\Sigma(\doteq)) (\sigma, \sigma) \) for each sort \( \sigma \in \text{Sort}(\Sigma) \). Consider a model \( \mathcal{M} \) of \( \Sigma(\doteq) \) in the sense of Def. 6.8 (§6.1.3), which (may not interpret \( \doteq_\sigma \) as equality but) additionally validates all the following formulae:

\[
(\forall x^\sigma)(x^\sigma \doteq_\sigma x^\sigma) \quad (\forall x^\sigma, y^\sigma)(x^\sigma \doteq_\sigma y^\sigma \Rightarrow A[x^\sigma/z^\sigma] \Rightarrow A[y^\sigma/z^\sigma])
\]

Consider in each \( \mathcal{M}(\sigma) \) the relation

\[ a \doteq_\sigma b \iff \mathcal{M}, [a/x^\sigma, b/y^\sigma] \models (x^\sigma \doteq_\sigma y^\sigma) \]

It easily follows from the above axioms on \( (\doteq)_\sigma \) that \( (\doteq)_\sigma \) is a family of equivalence relations on \( (\mathcal{M}(\sigma))_\sigma \) which is moreover compatible with all function and predicate symbols of \( \Sigma \). Then by quotienting each \( \mathcal{M}(\sigma) \) with \( \doteq_\sigma \) one obtains a model \( \mathcal{M}/\doteq \) such that for each sentence \( A \) (with equality) we have \( \mathcal{M} \models A \) (in the sense of first-order logic with equality). See e.g. [vD04, Proof of Lem. 3.1.11] for details.

6.4.4. Negative Translations for First-Order Predicate Logic with Equality

The negative translations mentioned in §6.2.3 can be straightforwardly adapted to equality. In particular, extend \( (\neg) \) (Def. 6.27) with

\[ (a^\sigma \doteq_\sigma b^\sigma) \neg := \neg (a^\sigma \doteq_\sigma b^\sigma) \]

\textbf{Theorem 6.65.} If \( \vdash A \) is derivable in NK\(_1\) with equality, then \( \vdash A^\neg \) is derivable in NJ\(_1\) with equality.

Theorem 6.65 is (an almost direct instance of) Cor. 7.69 (§7.3.4 below).

6.4.5. Proof-Terms for First-Order Predicate Logic with Equality

Similarly as in §6.3, we restrict to one-sorted signatures (and generalization to many-sorted signatures is straightforward).

A quite nice fact is that the equality rules of Fig. 15 (§6.4.2) admit decently behaved proof-terms. The typing rules are given in Fig. 16. They amount to extend the proof-terms for NJ\(_1\) over \( (\Sigma, \mathcal{V}) \) with

\[ t, u ::= \ldots \mid \text{eq}_I \ a \mid \text{eq}_E \ a \ b \ t \ u \]
6. First-Order Predicate Logic

where \(a, b \in \text{Ter}(\Sigma, \mathcal{V})\).

Beta-reduction is defined from the following obvious proof-reduction:

\[
\frac{\mathcal{E} \vdash \text{eq}_I \ a : a = a \quad \Pi}{\mathcal{E} \vdash \text{eq}_I \ a \ (\text{eq}_I \ a) \ u : A[a/x]} \quad \Downarrow_{\beta} \quad \Pi
\]

Technically it is actually convenient to let \(\Downarrow_{\beta}\) on untyped \(\lambda\)-terms be the contextual closure of the extension of \(\Downarrow_0\) (Fig. 14, §6.3.3) with

\[
\text{eq}_E \ a \ b \ (\text{eq}_I \ a) \ u \Downarrow_0 u
\]

All the statements of §6.3.3 remain true in \(\text{NJ}_1\) with equality, and we do not restate them. Note however that one should add \((\text{eq}_I \ a)\) among the \(\beta\)-normal forms in the empty context (Lem. 6.54). Normalization is discussed in §6.5.

### 6.4.6. On Term Extraction and Classical Logic

We come back on what is perhaps the most important property of \(\text{NJ}_1\), namely witness extraction from \(\text{NJ}_1\)-proofs of \(\forall \exists\)-statements (Cor. 6.41, §6.2.6), and discuss some of its salient aspects w.r.t. classical logic. We first restate the result for logic with equality.

**Corollary 6.66.** In \(\text{NJ}_1\) with equality, from a proof of \(\vdash (\forall x_1 \ldots x_n)(\exists y)A\) one can effectively compute a first-order term \(a = a(x_1, \ldots, x_n)\) and a proof of \(\vdash (\forall x_1 \ldots x_n)A[a/y]\).

Intuitionistic logic is crucial for Cor. 6.66. If \(\text{NJ}_1\) proves \(\vdash (\forall x_1 \ldots x_n)(\exists y)A\), then the latter is of course valid. But only assuming the validity of \((\forall x_1 \ldots x_n)(\exists y)A\) is not enough. In particular, given a valid closed formula \((\forall x_1 \ldots x_n)(\exists y)A\) and a model \(M\), the Axiom of Choice gives a function \(f : M^n \to M\) such that \((\forall x_1 \ldots x_n)A[f(x)/y]\) holds in \(M\). But there is no reason that \(f : M^n \to M\) is the interpretation of some term \(a = a(x_1, \ldots, x_n)\) over the signature under consideration! Moreover, even if it were, there is no reason to get the same term \(a\) for every model \(M\).

Actually (essentially) the best that classical logic can say in this case is the following version of the remarkable **Herbrand’s Theorem** ([Bus98a, 2.5.1], for which it is essential that equality can be axiomatized as in Rem. 6.61, §6.4.2).

**Theorem 6.67** (Herbrand). Let \((\forall x_1 \ldots x_n)(\exists y)A_0\) be a closed formula with equality, where \(A_0\) is quantifier-free (i.e. \(A_0\) contains no quantifier). In \(\text{NK}_1\) with equality, from a proof of \(\vdash (\forall x_1 \ldots x_n)(\exists y)A_0\) one can effectively compute a number \(k \geq 1\) and terms \(a_1, \ldots, a_k\) with variables among \(x_1, \ldots, x_n\) and such that

\[
\vdash (\forall x_1 \ldots x_n)\left(A_0[a_1/y] \lor \cdots \lor A_0[a_k/y]\right)
\]

We again insist on the effective character of Cor. 6.66 and Thm. 6.67, while provability in \(\text{NJ}_1\) and \(\text{NK}_1\) is undecidable (Thm. 6.35, §6.2.4). In particular, beware that the number \(k \in \mathbb{N}\) in Thm. 6.67 cannot be computed from \((\forall x_1 \ldots x_n)(\exists y)A_0\) alone ([Bus98a, 2.5.4], essentially because of the undecidability of first-order logic).
6. First-Order Predicate Logic

\[(a = b)^\circ := \text{unit} \]
\[(P(a_1, \ldots, a_n))^\circ := o \]
\[(A \Rightarrow B)^\circ := A^\circ \rightarrow B^\circ \]
\[(A \land B)^\circ := A^\circ \times B^\circ \]
\[(A \lor B)^\circ := A^\circ + B^\circ \]
\[\top^\circ := \text{unit} \]
\[\bot^\circ := \text{void} \]
\[((\forall x)A)^\circ := \iota \rightarrow A^\circ \]
\[((\exists x)A)^\circ := \iota \times A^\circ \]

Figure 17: The Translation \((-)^\circ\) of Formulae to Types.

6.5. Normalization

In this §6.5, we prove the strong normalization of the (typed) proof-terms for \(\text{NJ}_1\) with equality. As announced, we shall devise a translation \((-)^\circ\) from (typed) proof-terms to (typed) \(\lambda\)-terms with sums and products (§4.4.3) such that

\[t^\circ \triangleright^\gamma u^\circ \quad \text{whenever} \quad t \triangleright^\beta u\]

The strong normalization for \(\text{NJ}_1\) with equality will then be inferred from the strong normalization of the simply-typed \(\lambda\)-calculus with sums and products (Thm. 4.31, §4.4.4, a.k.a. Thm. 5.32, §5.5.3). Different proofs can be found in e.g. [SU06, §8.7], [TvD88b, Chap. 10, §8.4] or [Gal95].

The key idea in the definition of \((-)^\circ\) is to represent first-order terms by usual \(\lambda\)-terms, and to represent first-order formulae by simple types (with sums and products). Hence the translation \((-)^\circ\) depends on the first-order signature under consideration.

Fix a first-order signature \(\Sigma\) and a set of first-order variables \(V\) that (as for the proof-terms of §6.3 and §6.4.5) we assume to be one-sorted.

The translation \((-)^\circ\) targets simply-typed \(\lambda\)-terms with types over the grammar

\[T, U ::= \iota \mid o \mid U \rightarrow T \mid T \times U \mid T + U \mid \text{unit} \mid \text{void} \]

where

- \(\iota\) is a base type, which shall be used to type the \(\lambda\)-terms representing first-order terms over \((\Sigma, V)\); and
- \(o\) is a base type, which shall be used to represent the \(P \in \text{Pred}(\Sigma)\).

Figure 17 defines the translation \((-)^\circ\) of first-order formulae of \(\text{NJ}_1\) with equality to simple types over the above grammar. Note that \(A^\circ\) contains no first-order term, so that in particular \((A[a/x])^\circ = A^\circ\).

We now turn to terms. We assume given

- for each first-order variable \(x \in V\), a variable \(x^\circ \in \mathcal{X}\);
6. First-Order Predicate Logic

\[
x^o := x
\]
\[
(\lambda x.t)^o := \lambda x.t^o
\]
\[
(tu)^o := t^o u^o
\]
\[
(t, u)^o := (t^o, u^o)
\]
\[
(\pi_1 t)^o := \pi_1 t^o
\]
\[
(\pi_2 t)^o := \pi_2 t^o
\]
\[
(in_1 t)^o := in_1 t^o
\]
\[
(in_2 t)^o := in_2 t^o
\]
\[
(case \ t \ {in_1 x_1 \mapsto u_1 | \ in_2 x_2 \mapsto u_2})^o := case \ t^o \ {in_1 x_1 \mapsto u_1^o | \ in_2 x_2 \mapsto u_2^o}
\]
\[
(let \ (x, y) = t \ in \ u)^o := (\lambda p. u^o[\pi_1 p/x^o][\pi_2 p/y]^o)^o \ (p \notin \text{FV}(u^o))
\]
\[
(eq \ E \ a \ b \ t \ u)^o := (\lambda x. \lambda y. y)^o \ t^o \ u^o
\]

Figure 18: The Translation \((-)^o\) on Untyped Proof-Terms.

- for each \(f \in \text{Fun}(\Sigma)(n)\), a variable \(f^o \in X\) together with a type

\[
T_f := \underbrace{\iota \to \cdots \to \iota}_{n \text{ times}} \to \iota
\]

It then follows that for each first-order term \(a \in \text{Ter}(\Sigma, V)\) we obtain a typed \(\lambda\)-term

\[
\mathcal{I} \vdash a^o : \iota
\]

where \(\mathcal{I}\) is a first-order context, i.e. a typing context which consists only of declarations of the form \(x^o : \iota\) (where \(x \in V\)) or \(f^o : T_f\) (where \(f \in \text{Fun}(\Sigma)\)). The \(\lambda\)-term \(a^o\) is defined by induction on \(a \in \text{Ter}(\Sigma, V)\) as

\[
x^o := x^o \quad \text{and} \quad (f(a_1, \ldots, a_n))^o := f^o a_1^o \cdots a_n^o
\]

For the translation of proof-terms, we proceed in two steps. We first define a translation \((-)^o\) on untyped proof-terms in Fig. 18. Second, an easy induction on derivations shows that the translation \((-)^o\) preserves typing in the following sense, where given \(\mathcal{E} = x_1 : A_1, \ldots, x_n : A_n\), we write \(\mathcal{E}^o\) for \(x_1 : A_1^o, \ldots, x_n : A_n^o\).

**Lemma 6.68.** If \(\mathcal{E} \vdash t : A\) in NJ1 with equality, then there is a first-order context \(\mathcal{I}\) such that \(\mathcal{E}^o, \mathcal{I} \vdash t^o : A^o\).

**Proof.** Exercise!
We shall now show that the translation \((-)^0\) preserves \(\beta\)-reduction, in the sense that

\[ t^0 \xrightarrow{\beta} u^0 \quad \text{whenever} \quad t \xrightarrow{\beta} u \]

**Lemma 6.69 (Substitution).**

1. \((t[b/y])^0 = t^0[b^0/y^0]\
2. \((t[v/y])^0 = t^0[v^0/y]\

**Proof.** Exercise! \(\square\)

**Proposition 6.70.** If \(t \xrightarrow{\beta} u\) then \(t^0 \xrightarrow{\beta} u^0\).

**Proof.** Exercise! \(\square\)

We then obtain the strong normalization of the proof-terms of \(NJ_1\) with equality from the strong normalization of the simply-typed \(\lambda\)-calculus with sums and products (Thm. 4.31, §4.4.4, a.k.a. Thm. 5.32, §5.5.3).

**Corollary 6.71 (Strong Normalization).** If \(E \vdash t : A\) in \(NJ_1\) with equality, then \(t\) is strongly normalizing.

### 7. First-Order Arithmetic

First-order classical (“Peano”) and intuitionistic (“Heyting”) arithmetic (denoted resp. PA and HA) are fundamental systems, for reasons related to Gödel’s Incompleteness Theorems.

The key fact is that primitive recursion (and in particular finite sequences) can be represented in first-order arithmetic, which makes the latter a reference setting w.r.t. its provable statements on recursive functions and finitary data-structures.

Moreover, the very representation of primitive recursion allows for the usual Gödel’s coding of syntax, to the effect that proof-trees for first-order arithmetic can be represented within first-order arithmetic. The (usual) crucial consequence is that if first-order arithmetic is consistent, then it cannot prove its own consistency. This last fact puts first-order arithmetic at the basis of a hierarchy of systems (first-order, second-order and higher-order arithmetics, type theories, set theories, and fragments thereof)\(^{16}\) which (assuming their consistency) can be compared w.r.t. their proof-theoretic strength, i.e. w.r.t. their ability to prove the consistency of weaker systems, as well as w.r.t. which partial recursive functions they are able to prove to be total (references on this are [GLT89, TS00, Bee85]; see also [Sim10] for a different approach).

First-order arithmetics come under different presentations in the literature. For this reason, we begin in §7.1 with some key facts which are to be waited from virtually any **intuitionistic** first-order arithmetic.

\(^{16}\)First-order arithmetic as considered in this course is actually not the weakest system which can be taken as such a basis (see e.g. [Bus98b] for an introduction to weak systems of arithmetic).
7. First-Order Arithmetic

\[(\forall x)(\forall y)((\forall x)(\forall y)(\forall z)(x \neq y \land y \neq z \rightarrow x \neq z))\]

Figure 19: Basic Axioms on 0 and S.

\[(\forall x)(\forall y)(\forall z)(x \neq y \land y \neq z \rightarrow x \neq z)\]

Figure 20: Equality Axioms.

We then discuss in §7.2 a presentation of classical first-order Peano Arithmetic (PA) whose language contains one function symbol for each primitive recursive function.

The corresponding intuitionistic system, called Heyting Arithmetic (HA) is then discussed in §7.3, with a particular emphasis on its relation to PA and on its extraction results. Of particular importance is Kreisel’s Theorem 7.54 (§7.3.3), according to which HA and PA prove the same “Π₀²-sentences” (i.e. ∀∃-sentences over primitive recursive predicates), so that HA and PA prove the termination of the same algorithms.

In contrast with first-order logic (§6) we shall not look for a proper λ-calculus of proof-terms for HA. But there is an extension of the simply-typed λ-calculus associated to HA via a variant of the Curry-Howard correspondence. This typed λ-calculus, called Gödel’s System T, shall be discussed separately in §8.

7.1. Theories of Natural Numbers with Induction

Recall from Def. 6.26 (§6.2.2) that a classical (resp. intuitionistic) theory is a set Φ of sentences (i.e. closed formulae) of first-order predicate logic which is stable under classical (resp. intuitionistic) deduction.

In this §7 we shall be concerned with theories which contain at least the following.

Definition 7.1.

(1) We say that a first-order signature Σ is a signature with natural numbers if there is a sort \( t \in \text{Sort}(\Sigma) \) such that Σ contains the constant symbol 0 : \( t \) and the function symbol S : \( t \rightarrow t \).

(2) By a (classical resp. intuitionistic) theory of natural numbers we mean a (classical resp. intuitionistic) theory TH on a signature Σ with natural numbers such that TH proves all the formulae of Fig. 19 and of Fig. 20 (where f ∈ Fun(Σ)(\( t, \ldots, t; t \)) and P ∈ Pred(Σ)(\( t, \ldots, t \))).
(3) We say that a (classical resp. intuitionistic) theory of natural numbers \( \text{TH} \) has induction if \( \text{TH} \) proves all universal closures of the following, where \( A \) contains no disjunction (\( \lor \)):

\[
A[0/x] \Rightarrow (\forall x')(A \Rightarrow A[Sx/x]) \Rightarrow (\forall x')A
\]

**Notation 7.2.** The constant symbol 0 is intended to represent the natural number 0, while the function symbol \( S(\cdot) \) is intended to represent the successor function \( n \in \mathbb{N} \mapsto (n + 1) \in \mathbb{N} \).

1. We often write \( Sa \) instead of \( S(a) \) (as in Fig. 19).

2. Given a natural number \( n \in \mathbb{N} \), the **numeral** \( n \) is the (closed) first-order term defined by induction on \( n \) as \( 0 := 0 \) and \( n + 1 := S_n \).

**Remark 7.3.** The equality axioms of Fig. 20 are reminiscent from Rem. 6.61 (§ 6.4.2). It is well-known (see e.g. [vD04, § 2.10]) that these axioms are equivalent to the universal closures of

\[
a \equiv_i a \quad \text{and} \quad a \equiv_i b \Rightarrow A[a/x] \Rightarrow A[b/x]
\]

What may seem strange in Def. 7.1 is the condition that \( A \) contains no disjunction in the induction axiom

\[
A[0/x] \Rightarrow (\forall x')(A \Rightarrow A[Sx/x]) \Rightarrow (\forall x')A
\]

In the classical case, this is obviously not a restriction since disjunctions \( A \lor B \) can be defined as \( \neg(\neg A \land \neg B) \). In the intuitionistic case, this is due to the following well-known fact (see e.g. [TvD88a, Chap. 3, §3.2], also [SU06, Prop. 9.5.1]).

**Definition 7.4.** Assuming a signature with natural numbers, let

\[
A \lor B := (\exists z') \left[ (z \equiv_i 0) \Rightarrow A \right] \land (\neg(z \equiv_i 0) \Rightarrow B)
\]

**Proposition 7.5.** Let \( \text{TH} \) be an intuitionistic theory of natural numbers. Then \( \text{TH} \) proves the following:

1. \( A \Rightarrow A \lor B \)
2. \( B \Rightarrow A \lor B \)

If furthermore \( \text{TH} \) has induction, then \( \text{TH} \) proves

3. \( (A \lor B) \Rightarrow (A \Rightarrow C) \Rightarrow (B \Rightarrow C) \Rightarrow C \)
4. \( (A \lor B) \iff (A \lor B) \)

**Proof.** Exercise!
7. First-Order Arithmetic

We finally arrive at the fundamental fact that intuitionistic arithmetics prove the decidability of equality, namely:

\[(\forall x)(\forall y)(x =_i y \lor \neg(x =_i y))\]

This fact is at the basis of Kreisel’s Theorem 7.54 (§7.3.3) and of considerable further developments (see e.g. [TvD88a, TvD88b, Koh08]).

**Proposition 7.6.** Let \(TH\) be an intuitionistic theory of natural numbers. Then \(TH\) proves the following:

1. \((\forall x)(x =_i 0 \lor \neg(x =_i 0))\)
2. If furthermore \(TH\) has induction, then \(TH\) proves
   \((\forall x)(x =_i 0 \lor (\exists y)(x =_i Sy))\)
3. \((\forall x)(\forall y)(x =_i y \lor \neg(x =_i y))\)

**Proof.** Exercise!

**Corollary 7.7.** Intuitionistic theories of natural numbers with induction prove

1. \((\forall x)(x =_i 0 \lor \neg(x =_i 0))\)
2. \((\forall x)(x =_i 0 \lor (\exists y)(x =_i Sy))\)
3. \((\forall x)(\forall y)(x =_i y \lor \neg(x =_i y))\)

7.2. Peano Arithmetic

Peano Arithmetic is usually defined as the (classical) first-order theory (denoted \(\text{PA}_0\) in the following) of natural numbers with induction (§7.1) and with function symbols \((-\) \(+\), \((-\) \(*\)) for resp. addition and multiplication on natural numbers, together with their defining equations.

However, it is well-known (and it follows from results essentially due to Gödel) that \(\text{PA}_0\) can be conservatively extended with function symbols for primitive recursive functions. This results in a system (denoted \(\text{PA}\) in the following) whose intuitionistic counterpart, called **Heyting Arithmetic** (denoted \(HA\) and to be defined in §7.3), is often considered to be the good version of intuitionistic first-order arithmetic (besides [SU06, §9.5], see e.g. [TvD88a, Chap. 3, §3], [Tro73, §1.3] and [Koh08, §3.2]).

We shall thus begin in §7.2.1 with some reminder on primitive recursive functions, and in particular on the representation of partial recursive functions (§7.2.2). The language and axioms of first-order arithmetic are presented in §7.2.3 and §7.2.4 respectively. Our version of Peano Arithmetic (PA) is then defined in §7.2.5, while §7.2.6 is a reminder on the main results toward **Gödel’s Incompleteness Theorems**, which also introduces the concept of **provably total function**, an important notion for comparing the proof-theoretic strength (i.e. provability) of theories containing arithmetic, in particular in relation to normalization of typed \(\lambda\)-calculi (see e.g. [GLT89, TS00, Bee85]).
7. First-Order Arithmetic

This §7.2 is mostly based on [SU06, §9], but we also refer to [vD04, BBJ07] for material on primitive recursive functions and on Gödel’s Incompleteness Theorems. We also refer to [Odi99] for the modicum of recursion theory we shall need.

### 7.2.1. Primitive Recursive Functions

We recall the definition of the primitive recursive functions. See [vD04, §7.1], [TvD88a, Chap. 3, §1] or [SU06, §A3] (also [BBJ07, §6.1]).

#### Notation 7.8. We use the following notations.

1. If \( f \) is a function from \( \mathbb{N}^k \) to \( \mathbb{N} \) (\( k \geq 0 \)), then we write \( f : \mathbb{N}^k \to \mathbb{N} \).

2. **Composition**: Given \( f : \mathbb{N}^m \to \mathbb{N} \) and, \( g_i : \mathbb{N}^k \to \mathbb{N} \) (\( 1 \leq i \leq m \)), then define \( f \circ \langle g_1, \ldots, g_m \rangle : \mathbb{N}^k \to \mathbb{N} \) as
   \[
   (f \circ \langle g_1, \ldots, g_m \rangle)(n_1, \ldots, n_k) := f(g_1(n_1, \ldots, n_k), \ldots, g_m(n_1, \ldots, n_k))
   \]

3. **Primitive Recursion**: Given \( f : \mathbb{N}^k \to \mathbb{N} \) and \( g : \mathbb{N}^{k+2} \to \mathbb{N} \), we write \( \text{Iter}(f, g) : \mathbb{N}^{k+1} \to \mathbb{N} \) for the function defined as
   \[
   \text{Iter}(f, g)(n_1, \ldots, n_k, 0) := f(n_1, \ldots, n_k)
   \]
   \[
   \text{Iter}(f, g)(n_1, \ldots, n_k, n + 1) := g(n_1, \ldots, n_k, n, \text{Iter}(f, g)(n_1, \ldots, n_k, n))
   \]

4. The **Zero** function \( \text{Zero}^k : \mathbb{N}^k \to \mathbb{N} \) is
   \[
   \text{Zero}^k(n_1, \ldots, n_k) := 0
   \]

5. The **Successor** function \( \text{Succ} : \mathbb{N} \to \mathbb{N} \) is
   \[
   \text{Succ}(n) := n + 1
   \]

6. If \( 1 \leq i \leq k \), the **Projection** function \( \pi_i^k : \mathbb{N}^k \to \mathbb{N} \) is
   \[
   \pi_i^k(n_1, \ldots, n_k) := n_i
   \]

#### Definition 7.9 (Primitive Recursive Function).

The set \( \text{PR} \) of **primitive recursive functions** is the smallest subset of \( \bigcup_{k \in \mathbb{N}} \mathbb{N}^k \) which is closed under the following rules:

\[
\begin{align*}
\text{Zero}^k & \in \text{PR}(k) & \text{Succ} & \in \text{PR}(1) & \pi_i^k & \in \text{PR}(k) \\
f \in \text{PR}(m) & & g_1 \in \text{PR}(k) & & \ldots & & g_m \in \text{PR}(k) \\
f \circ \langle g_1, \ldots, g_m \rangle & \in \text{PR}(k) & & f \in \text{PR}(k) & & g \in \text{PR}(k+2) \\
& & & \text{Iter}(f, g) & \in \text{PR}(k+1)
\end{align*}
\]

where
\[
\text{PR}(k) := \{ f \in \text{PR} \mid f : \mathbb{N}^k \to \mathbb{N} \}.
\]
Example 7.10. Addition (\(+\)) and multiplication (\(\times\)) on natural numbers are of course primitive recursive:

\[
\begin{align*}
n + 0 &= n \\
n + (m + 1) &= (n + m) + 1 \\
n \times 0 &= 0 \\
n \times (m + 1) &= n + (n \times m)
\end{align*}
\]

Example 7.11. The following primitive recursive functions come in particularly handy for intuitionistic arithmetic (see e.g. [vD04, §7.1] or [TvD88a, Chap. 3, §1.3]):

\[
\begin{align*}
sg(0) &= 1 \\
sg(n + 1) &= 0 \\
pred(0) &= 0 \\
pred(n + 1) &= n \\
n - 0 &= n \\
n - (m + 1) &= \text{pred}(n - m) \\
|n - m| &= (n - m) + (m - n)
\end{align*}
\]

Note that

\[
n - m = \begin{cases} n - m & \text{if } n \geq m \\ 0 & \text{otherwise} \end{cases}
\]

so that \(|n - m| = 0\) iff \(n = m\).

Example 7.12. Following [SU06, §A3] (also [TvD88a, Chap. 3, §1.8]) we assume a given primitive recursive bijection \(<-, ->: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}\) with primitive recursive inverses \(\pi_1, \pi_2\) such that

\[
\pi_1(n, m) = n \quad \text{and} \quad \pi_2(n, m) = m
\]

Definition 7.13. A relation \(P \subseteq \mathbb{N}^k\) is primitive recursive if its characteristic function

\[
\chi_P : (n_1, \ldots, n_k) \mapsto \begin{cases} 1 & \text{if } (n_1, \ldots, n_k) \in P \\ 0 & \text{otherwise} \end{cases}
\]

is primitive recursive.

Notation 7.14. We often write \(P(x_1, \ldots, x_k)\) to mean \(P \subseteq \mathbb{N}^k\), and \(P(n_1, \ldots, n_k)\) (where \(n_1, \ldots, n_k \in \mathbb{N}\)) to mean \((n_1, \ldots, n_k) \in P\).

7.2.2. Representation of Computable Functions

Primitive recursion allows for a neat treatment of Church-Turing computability. Besides [SU06, §A3], we refer to e.g. [TvD88a, Chap. 2, §4 & §7], [vD04, §7.2] or [BBJ07, §6 & §8].

Theorem 7.15 (Kleene’s T Predicate). There exist

(a) for each partial recursive function \(f : \mathbb{N} \rightarrow \mathbb{N}\), a natural number \(e_f \in \mathbb{N}\) (called the Kleene index of \(f\), [vD04, §7.2]) and

(b) a primitive recursive relation \(T(x, y, z, w)\)

such that
• for every partial recursive \( f : \mathbb{N} \to \mathbb{N} \) and every \( n,m \in \mathbb{N} \), we have \( f(n) = m \) if and only if there is some \( k \in \mathbb{N} \) such that \( T(e_f, n, m, k) \).

**Remark 7.16.** Theorem 7.15 can be obtained from the usual correspondence between partial recursive functions and Turing machines, together with the existence of a universal Turing machine (see e.g. [BBJ07, §6 & §8]). In particular, to each partial recursive function \( f : \mathbb{N} \to \mathbb{N} \) corresponds a Turing machine \( M_f \) (see e.g. [BBJ07, Thm. 8.2]), and instead of the predicate \( T(x, y, z, w) \) of Thm. 7.15, one may have considered a primitive recursive predicate \( T(x, y, z) \) such that

\[
T(e_M, n, k) \text{ holds if and only if } k \text{ codes a terminating computation of the Turing machine } M \text{ on input } n.
\]

**Theorem 7.17** (The Halting Problem (Turing)). The following problem is undecidable:

• Given a partial recursive function \( f \) and \( n \in \mathbb{N} \), decide whether there exists some \( m \in \mathbb{N} \) such that \( f(n) = m \).

**Corollary 7.18.** The following problem is undecidable:

• Given a primitive recursive predicate \( P(x_1, \ldots, x_k, y_1, \ldots, y_\ell) \) and \( n_1, \ldots, n_k \in \mathbb{N}, \)

decide whether there exist some \( m_1, \ldots, m_\ell \in \mathbb{N} \) such that \( P(n_1, \ldots, n_k, m_1, \ldots, m_\ell) \).

**Proof.** Exercise! \(
\square
\)

### 7.2.3. The Language of First-Order Arithmetic

We consider a signature \( \Sigma_{\text{PR}} \) for first-order arithmetic with one function symbol for each primitive recursive function. In §7.2.4 below, we shall then postulate appropriate (equational) axioms on these function symbols. But doing this in an effective way requires some care, essentially because testing equality of primitive recursive functions is undecidable (see Prop. 7.38, §7.2.7 below). We shall actually not merely assume one function symbol \( f \) for each primitive function \( f \in \text{PR} \), but rather assume one function symbol \( f_T \) for each derivation tree \( T \) that ensures \( f \in \text{PR} \) according to the rules of Def. 7.9 (§7.2.1).

The equational axioms on \( f_T \) will then correspond to the equalities naturally associated to each rule of Def. 7.9 (see Notation 7.8).

We formally proceed as follows. Let \( T_{\text{PR}} \) be the set of finite derivation trees built according to the rules of Def. 7.9 (§7.2.1). Let \( T \in T_{\text{PR}} \) be such a derivation tree. By definition, \( T \) proves \( f \in \text{PR}(k) \) for some \( f : \mathbb{N}^k \to \mathbb{N} \) and some \( k \in \mathbb{N} \). We associate to \( T \) a function symbol \( f_T \) of arity \( k \).

We assume no predicate symbol besides equality (§6.4.1).

**Definition 7.19.** The signature \( \Sigma_{\text{PR}} \) is the one-sorted signature with no predicate symbol and with function symbols

\[
\begin{align*}
\text{Fun}(\Sigma_{\text{PR}}) & := \bigcup_{k \in \mathbb{N}} \text{Fun}(\Sigma_{\text{PR}})(k) \\
\text{Fun}(\Sigma_{\text{PR}})(k) & := \{ f_T \mid T \in T_{\text{PR}} \text{ proves that } f \in \text{PR}(k) \}
\end{align*}
\]
7. First-Order Arithmetic

The language of first-order arithmetic is the language of (one-sorted) first-order logic with equality over \( \Sigma_{\text{PR}}\) (§6.4). In other words, assuming a set \( \mathcal{V} \) of first-order variables, the formulae of first-order arithmetic are given by:

\[
A, B ::= (a \doteq b) \mid \top \mid \bot \mid A \land B \mid A \lor B \mid A \rightarrow B \\
\mid (\forall x)A \mid (\exists x)A
\]

where \( a, b \in \text{Ter}(\Sigma_{\text{PR}}, \mathcal{V}) \).

Notation 7.20.

(1) If \( T \) is \( \text{Zero}_0 \in \text{PR}(0) \) then \( f_T \) is written 0.

(2) If \( T \) is \( \text{Succ} \in \text{PR}(1) \) then \( f_T \) is written \( S \).

(3) If \( T \) is \( \pi_k^i \in \text{PR}(k) \) then \( f_T \) is written \( \pi_k^i \).

Notation 7.21 (Numerals). Hence \( \Sigma_{\text{PR}} \) is a signature with natural numbers in the sense of §7.1. In particular, we assume Notation 7.2, and to each \( n \in \mathbb{N} \) corresponds the numeral \( n = \underbrace{S \ldots S}_n \cdot 0 \).

7.2.4. The Axioms of First-Order Arithmetic

The axioms of first-order arithmetic \( \text{Ax}_{\text{PR}} \) consist of the following rules.

(1) **Non-Confusion.**

\[
\Delta \vdash (\forall x) \neg(Sx \doteq 0)
\]

(2) **Induction Scheme.** For each formula \( A \),

\[
\Delta \vdash A[0/x] \rightarrow (\forall y)(A[y/x] \rightarrow A[Sy/x]) \rightarrow (\forall x)A
\]

(3) **Equational Axioms.** We associate equational axioms to trees \( T \in T_{\text{PR}} \) as follows.

- If \( T \) is \( \text{Zero}_k \in \text{PR}(k) \) \( (k \geq 1) \) then we have the axiom

\[
\Delta \vdash (\forall x_1, \ldots, x_k)(f_T(x_1, \ldots, x_k) \doteq 0)
\]

99
7. First-Order Arithmetic

• If \( T \) is

\[
\pi^k_i \in \text{PR}(k)
\]

then we have the axiom

\[
\Delta \vdash (\forall x_1, \ldots, x_k) (\pi^k_i(x_1, \ldots, x_k) \equiv x_i)
\]

• If \( T \) is

\[
\begin{array}{cccc}
\vdots & \vdots & \vdots \\
g \in \text{PR}(m) & \mathcal{U} & \nu_1 & \cdots & \nu_m \\
\mathcal{V}_1 & h_1 \in \text{PR}(k) & \cdots & h_m \in \text{PR}(k) \\
g \circ (h_1, \ldots, h_m) \in \text{PR}(k)
\end{array}
\]

then we have the axiom

\[
\Delta \vdash (\forall x_1, \ldots, x_k) (f_T(x_1, \ldots, x_k) \equiv f_U(f_{\nu_1}(x_1, \ldots, x_k), \ldots, f_{\nu_m}(x_1, \ldots, x_k)))
\]

• If \( T \) is

\[
\begin{array}{c}
\vdots \\
g \in \text{PR}(k) \\
\nu \in \text{PR}(k+2)
\end{array}
\]

\[
\text{Iter}(g, h) \in \text{PR}(k+1)
\]

then we have the axioms

\[
\Delta \vdash (\forall x_1, \ldots, x_k) (f_T(x_1, \ldots, x_k, 0) \equiv f_U(x_1, \ldots, x_k))
\]

\[
\Delta \vdash (\forall x_1, \ldots, x_k, y) (f_T(x_1, \ldots, x_k, Sy) \equiv f_U(x_1, \ldots, x_k, y, f_T(x_1, \ldots, x_k, y)))
\]

7.2.5. First-Order Peano Arithmetic

Definition 7.22 (First-Order Peano Arithmetic). **First-order Peano Arithmetic (PA)** is \( \text{NK}_1 \) with equality over \( (\Sigma_{\text{PR}}, \nu) \) (§6.4.2) extended by all the rules of \( \text{Ax}_{\text{PR}} \).

Notation 7.23. We also write \( \text{PA} \) for the theory induced by \( \text{PA} \), i.e. the set of all closed formulae \( A \) such that \( \vdash A \) in \( \text{PA} \).

Notation 7.24. Once the axioms of first-order arithmetic are set, we notationally forget about derivation trees \( T_f \) proving \( f \in \text{PR} \), and directly write \( f \) instead of \( T_f \). This in particular applies to all primitive recursive functions of §7.2.1 and §7.2.2.
Example 7.25. Recall the primitive recursive function $\text{pred} : \mathbb{N} \to \mathbb{N}$ of Ex. 7.11 (§7.2.1), with equations

$$\text{pred}(0) = 0 \quad \text{and} \quad \text{pred}(n + 1) = n$$

The function $\text{pred}$ can be represented in $\text{PA}$ via the tree

$$
\begin{array}{c}
0 \in \text{PR}(0) \\
\pi_1^2 \in \text{PR}(2)
\end{array}
\quad \text{Iter}(0, \pi_1^2)(x) \in \text{PR}(1)
$$

so that the following rules are derivable in $\text{PA}$:

$$\Delta \vdash \text{pred}(0) \equiv 0 \quad \text{and} \quad \Delta \vdash (\forall x)(\text{pred}(Sx) \equiv x)$$

Remark 7.26. Note that $\text{Ax}_{\text{PR}}$ does not include the rule

$$\Delta \vdash (\forall x)(\forall y)(Sx \equiv Sy \Rightarrow x \equiv y)$$

expressing the injectivity of the successor function. But this rule is derivable from the equality axioms together with the rule

$$\Delta \vdash (\forall x)(\text{pred}(Sx) \equiv x)$$

of Ex. 7.25. In particular, $\text{PA}$ is a classical theory of natural numbers with induction in the sense of §7.1.

Notation 7.27. If $P \subseteq \mathbb{N}^k$ is a primitive recursive relation (Def. 7.13, §7.2.1), we write $P(a_1, \ldots, a_k)$ for a formula $\chi_P(a_1, \ldots, a_k) \equiv 1$ (where $\chi_P$ is the characteristic function of $P$). We moreover call $P(x_1, \ldots, x_k)$ a primitive recursive predicate.

Definition 7.28. The standard model of $\text{PA}$ is the set of natural numbers equipped with the obvious interpretation of each function symbol of $\Sigma_{\text{PR}}$ (so that each term $a(x_1, \ldots, x_k)$ induces a primitive recursive function $J_a : \mathbb{N}^k \to \mathbb{N}$ in the obvious way).

$A$ (closed) formula $A$ is true if $A$ is valid (Def. 6.11 §6.1.3) in the standard model.

Remark 7.29. Our axiomatization of Peano Arithmetic is in accordance with [TvD88a, Chap. 3, §3.4] (see also [Koh08, §3.2]). But other usual definitions of $\text{PA}$ do not include all primitive recursive functions from the start (besides [SU06, §9.2], see e.g. [vD04, §7.4]). Typically one considers (classical) first-order logic with equality over a (one-sorted) signature with natural numbers (§7.1) and binary function symbols $(-) + (-)$, $(-) \times (-)$ together with the axioms of Non-Confusion (7.2.4.(1)) and Induction (7.2.4.(2)) as well as the defining equality axioms for $+, \times$ (as in Ex. 7.10, §7.2.1). Write PA$_0$ for the resulting system.

The difference is inessential since our version of $\text{PA}$ is conservative over PA$_0$, i.e. for every formula $A$ of PA$_0$, we have $\vdash A$ in PA$_0$ if and only if $\vdash A$ in $\text{PA}$ (Thm. 7.32, §7.2.6 below, see e.g. [SU06, Thm. 9.4.5]).
7. First-Order Arithmetic

7.2.6. Representation and Incompleteness

We now recall some well-known facts on the representation of functions in arithmetic. Of crucial importance is the notion of provably total function (Def. 7.31). But we shall also mention important facts of general interest, in particular Gödel’s Incompleteness Theorems, and the conservativity of PA over PA₀ (Thm. 7.32), see Rem. 7.29 (§7.2.5) above. Most of this §7.2.6 is based on [SU06, §9], but we mention other pertinent references in the text.

We begin with the following usual fact on the representation of total recursive functions in (classical) arithmetic. Write \((\exists! z)B(z)\) for \((\exists z)(B(z) \land (\forall w)(B(w) \Rightarrow w = z))\).

**Theorem 7.30.** The following are equivalent for a function \(f : \mathbb{N}^k \rightarrow \mathbb{N}\):

- The function \(f\) is total recursive.
- There exists a formula \(A(x_1, \ldots, x_k, y)\) of PA₀ (with free variables as displayed) such that
  1. for all \(n_1, \ldots, n_k, m \in \mathbb{N}\), we have \(f(n_1, \ldots, n_k) = m\) if and only if PA₀ proves \(\vdash A(n_1, \ldots, n_k, m)\); and
  2. PA₀ proves \(\vdash (\forall x_1 \cdot \cdot \cdot x_n)(\exists! y)A(x_1, \ldots, x_n, y)\).

Theorem 7.30 is essentially due to Gödel, see [SU06, Prop. 9.4.2 & Thm. 9.4.3] (see also [vD04, §7.5]).

Beware that Thm. 7.30 does not mean that the classically provable \(\forall\exists!\) -statements of arithmetic can be witnessed by computable functions! The most fruitful notion of representation of function in arithmetic is the following. Recall Kleene’s T predicate of Thm. 7.15 (7.2.2).

**Definition 7.31 (Provably Total Function).** Let TH be a (classical or intuitionistic) theory over the signature \(\Sigma_{PR}\) of arithmetic (Def. 7.19, §7.2.3). A partial recursive function \(f : \mathbb{N} \rightarrow \mathbb{N}\) is provably total in TH if TH proves \(\forall x)(\exists! z)T(f, x, \pi_1 z, \pi_2 z)\).

While the notion of representation of Thm. 7.30 is not very attractive from the perspective of witness extraction (because of condition (i)), it (almost directly) gives the conservativity of PA₀ over PA (Rem. 7.29, §7.2.5), see [SU06, Thm. 9.4.5]

**Theorem 7.32 (Conservativity).** PA is conservative over PA₀.

**Remark 7.33.** Using [SU06, Thm. 9.4.4], Thm. 7.30 can be refined so as to attribute a PA₀-formula \(A_{f_T}(x_1, \ldots, x_k, y)\) to each tree \(T\) proving \(f \in PR(k)\) in such a way that PA proves

\[\vdash (\forall x_1 \cdot \cdot \cdot x_k)(\forall y)(f_T(x_1, \ldots, x_k) \Rightarrow y \Leftrightarrow A_{f_T}(x_1, \ldots, x_k, y))\]

This in particular implies that PA proves all true equalities of the form \(a = b\) where \(a, b\) are closed terms.

Theorem 7.30 is also crucial for Gödel’s (first) Incompleteness Theorem 7.35, essentially because it implies that for every recursive \(R \subseteq \mathbb{N}^k\), there is a formula \(A(x_1, \ldots, x_k)\) of PA₀ such that:

102
7. First-Order Arithmetic

- for every \( n_1, \ldots, n_k \in \mathbb{N} \), we have \( (n_1, \ldots, n_k) \in R \) if and only if \( \text{PA}_0 \) proves \( A(n_1, \ldots, n_k) \).

Gödel’s Incompleteness also relies on the arithmetization of syntax, i.e. the representation of syntactic objects (terms, formulae, proofs, etc.) by natural numbers. Besides [SU06, §9.3], see e.g. [vD04, §7.6] or [BBJ07, §15].

**Theorem 7.34** (Gödel Numbers). There exist

(a) a primitive recursive predicate \( \text{Proof}(x, y) \), and

(b) for each formula \( A \) of \( \text{PA}_0 \) a natural number \( \uparrow A \) (called the Gödel number of \( A \), [SU06, §9.3])

such that

- for each formula \( A \) of \( \text{PA}_0 \), we have \( \vdash A \) in \( \text{PA}_0 \) if and only if \( \text{Proof}(k, \uparrow A) \) for some \( k \in \mathbb{N} \).

The following is Gödel’s First Incompleteness Theorem (see e.g. [vD04, §7.7] or [BBJ07, §17]).

**Theorem 7.35** (Gödel). Assuming that \( \text{PA}_0 \) is consistent, there is a sentence \( Z \) such that \( \text{PA}_0 \) proves neither \( \vdash Z \) nor \( \vdash \neg Z \).

Gödel’s Second Incompleteness Theorem is a non-trivial strengthening of Thm. 7.35 according to which the undecidable sentence \( Z \) can be taken to be \( (\forall z)\neg \text{Proof}(z, \uparrow \bot) \), where \( \text{Proof}(x, y) \) stands for the formula of \( \text{PA}_0 \) which represents the primitive recursive relation \( \text{Proof} \) via Thm. 7.34. We refer to [BBJ07, Thm. 18.1] (see also [SU06, Thm. 9.3.3]).

**Theorem 7.36** (Gödel). Assuming that \( \text{PA}_0 \) is consistent, neither \( (\exists z)\text{Proof}(z, \uparrow \bot) \) nor \( \neg(\exists z)\text{Proof}(z, \uparrow \bot) \) is provable in \( \text{PA}_0 \).

It is immediate from the conservativity of \( \text{PA} \) over \( \text{PA}_0 \) (Thm. 7.32) that \( \text{PA} \) is also incomplete.

**Corollary 7.37.** Assuming that \( \text{PA} \) is consistent, \( \text{PA} \) proves neither \( (\exists z)\text{Proof}(z, \uparrow \bot) \) nor \( \neg(\exists z)\text{Proof}(z, \uparrow \bot) \).

### 7.2.7. A Classical Arithmetic of True Equalities

The definition of \( \text{PA} \) in §7.2.5 may seem a bit contrived because of the equational axioms 7.2.4.(3). It is tempting to rather consider the following system \( \text{PA}^* \) of first-logic with equality over the signature with one function symbol \( f \) of arity \( k \) for each primitive recursive function \( f : \mathbb{N}^k \to \mathbb{N} \). The axioms of \( \text{PA}^* \) are Non-Confusion (7.2.4.(1)) and Induction (7.2.4.(2)), together with the following

\[
\frac{[a] = [b]}{\Delta \vdash (x_1, \ldots, x_k)(a \equiv b)}
\]
where \(a, b\) have variables among \(x_1, \ldots, x_k\) and \([a], [b]\) stand for the obvious interpretations of \(a, b\) as primitive recursive functions \(N^k \to N\).

Systems defined in this way may be interesting for concrete applications of proof-theory (see e.g. [Koh08, §3.5]). But beware that \(\text{PA}^*\) is not conservative over \(\text{PA}_0\) (assuming the consistency of \(\text{PA}_0\)), since \(\text{PA}^*\) proves \((\forall z)(\neg \text{Proof}(z, \lceil \bot \rceil))\). Moreover, \(\text{PA}^*\) has a non-recursive set of axioms because of the following.

**Proposition 7.38.** The following problem is undecidable:

- Given primitive recursive functions \(f, g : N^k \to N\), decide whether \(f(n_1, \ldots, n_k) = g(n_1, \ldots, n_k)\) for all \(n_1, \ldots, n_k \in N\).

Proposition 7.38 essentially follows from the undecidability of the Halting Problem (Thm. 7.17, §7.2.2). But note that this requires an effective representation of the primitive recursive functions. Beware that Kleene’s indexes (in the sense of Thm. 7.15, §7.2.2) are not a recursive subset of the set of Kleene’s indexes of all partial recursive functions (a direct consequence of Rice’s Theorem, see e.g. [AC98, Cor. A1.3.2], see also [Odi99, Thm. II.2.9]). On the other hand, the construction of Gödel’s numbers of formulae in Thm. 7.34 §7.2.6 (see e.g. [vD04, §7.6]) can readily be adapted to yield the following, based on the signature \(\Sigma_{\text{PR}}\) of Def. 7.19 (§7.2.3).

**Assumption 7.39.** We assume given

(a) for each \(f_T \in \text{Fun}(\Sigma_{\text{PR}})(k)\), a natural number \(\lceil f_T \rceil\), and

(b) a primitive recursive function \(\text{const} : N \to N\), and

(c) for each \(k, \ell \in N\) a primitive recursive function \(\text{comp}_{k, \ell} : N^{k+1} \to N\) such that

(i) we have \(\text{const}(n) = \lceil f_T \rceil\) where \(T\) proves \((\neg \rightarrow n) \in \text{PR}(1)\), and

(ii) we have \(\text{comp}_{k, \ell}(\lceil f_T \rceil, \lceil f_{U_1} \rceil, \ldots, \lceil f_{U_k} \rceil) = \lceil f_V \rceil\) where \(V\) proves \(f \circ (g_1, \ldots, g_k) \in \text{PR}(\ell)\) assuming \(T\) proves \(f \in \text{PR}(k)\) and \(U_i\) proves \(g_i \in \text{PR}(\ell)\) for \(i = 1, \ldots, k\).

We can now prove Prop. 7.38.

**Proof.** It clearly follows from Ex. 7.11 (§7.2.1) that we can consider the sub-problem of deciding whether \(f(n_1, \ldots, n_k) = 0\) for all \(n_1, \ldots, n_k \in N\), in terms of the Gödel number \(\lceil f_T \rceil\) such that \(T\) proves \(f \in \text{PR}(k)\). Assume toward a contradiction that the problem is decidable for \(k = 2\), so that we have a total recursive function \(g : N \to N\) such that \(g(\lceil f_T \rceil) = 0\) iff \(T\) proves \(f \in \text{PR}(2)\) with \(f(n, m) = 0\) for all \(n, m \in N\).

Let \(t : N^4 \to N\) be the characteristic function of Kleene’s \(T\) predicate (Thm. 7.15, §7.2.2). For each \(n, m \in N\) the function \((k, \ell) \mapsto t(n, m, k, \ell)\) is primitive recursive, and it follows from our Assumption 7.39 that the following function is primitive recursive:

\[ h : (n, m) \mapsto \lceil f_T \rceil \text{ where } T \text{ proves } ((k, \ell) \mapsto t(n, m, k, \ell)) \in \text{PR}(2) \]
7. First-Order Arithmetic

Hence the function

\[(n, m) \mapsto (g \circ h)(n, m)\]

is total recursive.

Given a partial recursive \(f : \mathbb{N} \to \mathbb{N}\) and \(n \in \mathbb{N}\), we have

\[ (g \circ h)(e_f, n) = 0 \text{ iff } t(e_f, n, -, -) \text{ is everywhere null} \]
\[ \quad \text{iff for all } m, k \in \mathbb{N} \text{ we have } (e_f, n, m, k) \notin T \]
\[ \quad \text{iff for all } m \in \mathbb{N}, f(n) \neq m \]

But it is undecidable from \(e_f\) and \(n\) whether there is some \(m \in \mathbb{N}\) such that \(f(n) = m\). \(\square\)

7.3. Heyting Arithmetic

We let Heyting Arithmetic (HA) be the intuitionistic version of Peano Arithmetic with function symbols for primitive recursive functions (PA, §7.2.5). This follows [SU06, §9.5] (see also [TvD88a, Chap. 3, §3], [Tro73, §1.3] and [Koh08, §3.2]).

**Definition 7.40** (First-Order Heyting Arithmetic). The **First-order Heyting Arithmetic** (HA) is \(NJ_1\) with equality (§6.4.2) over the signature \(\Sigma_{PR}\) (§7.2.3), extended by all the rules of \(Ax_{PR}\) (§7.2.4).

**Notation 7.41.** Similarly as for Peano arithmetic (§7.2.5), we also write HA for the theory induced by HA, i.e. the set of all closed formulae \(A\) such that \(\vdash A\) in HA.

Sections 7.3.1 and 7.3.2 present basic properties of HA, essentially extending §7.1 with the benefits of having functions symbols for primitive recursive functions. The main properties of HA are then discussed in §7.3.3, most notably Kreisel’s Theorem 7.54, according to which HA and PA prove the same “\(\Pi^0_2\)-sentences” (i.e. \(\forall\exists\)-sentences over primitive recursive predicates), and in particular prove the termination of the same algorithms. Finally, a proof of Kreisel’s Theorem is presented in §7.3.4, using a technique originally due to Friedman.

7.3.1. Examples and Basic Properties

First note that Rem. 7.26 (§7.2.5) applies to HA, so that HA proves the axiom

\[(\forall x)(\forall y)(Sx \equiv Sy \Rightarrow x \equiv y)\]

of Fig. 19 (§7.1). Hence, HA is an intuitionistic theory of natural numbers with induction (Def. 7.1, §7.1). We thus get the following Prop. 7.42 and Prop. 7.43 from resp. Cor. 7.7 and Prop. 7.5 (§7.1).

**Proposition 7.42.** HA proves the following:

1. \((\forall x)(x \equiv 0 \lor \neg(x \equiv 0))\)
2. \((\forall x)(x \equiv 0 \lor (\exists y)(x \equiv Sy))\)
Proposition 7.43. Given formulae \( A, B \), let
\[
A ∨ B := (∃z)[((z = 0) ⇒ A) ∧ (¬(z = 0) ⇒ B)]
\]
(where \( z \notin \text{FV}(A) \cup \text{FV}(B) \)). Then HA proves the following:

(1) \( A ⇒ A ∨ B \)

(2) \( B ⇒ A ∨ B \)

(3) \( (A ∨ B) ⇒ (A ⇒ C) ⇒ (B ⇒ C) ⇒ C \)

(4) \( (A ∨ B) ⇔ (A \lor B) \)

Example 7.44. HA has in particular function symbols for addition \((-) + (-)\) and multiplication \((-) \times (-)\) (Ex. 7.10, §7.2.1), on which HA proves

\[
\begin{align*}
x + 0 & \doteq x \\
x + S(y) & \doteq S(x + y) \\
x \times 0 & \doteq 0 \\
x \times S(y) & \doteq x + (x \times y)
\end{align*}
\]

Moreover, HA proves the following:

(1) \( (∀y)(0 + y \doteq y) \)

(2) \( (∀x)(∀y)(x + y \doteq y + x) \)

(3) \( (∀x)(∀y)(∀z)((x + y) + z \doteq x + (y + z)) \)

(4) \( (∀x)(∀y)(x + y \doteq 0 ⇒ y \doteq 0) \)

(5) \( (∀x)(∀y)(x + y \doteq y ⇒ x \doteq 0) \)

PROOF. Exercise! ∎

Definition 7.45. Let
\[
\begin{align*}
x \leq y & := (∃z)(x + z \doteq y) \\
x < y & := (x \leq y) ∧ ¬(x \doteq y)
\end{align*}
\]

Lemma 7.46. HA proves the following:

(1) \( (∀x)(x \leq x) \)

(2) \( (∀x)(∀y)(∀z)(x \leq y ⇒ y \leq z ⇒ x \leq z) \)

(3) \( (∀x)(∀y)(x \leq y ⇒ y \leq x ⇒ x \doteq y) \)

(4) \( (∀x)¬(x < x) \)

(5) \( (∀x)(∀y)(∀z)(x < y ⇒ y < z ⇒ x < z) \)
7. First-Order Arithmetic

(6) $(\forall x)(\forall y) (x \leq y \iff (x \equiv y \lor x < y))$

(7) $(\forall x)(x \leq 0 \Rightarrow x \equiv 0)$

(8) $(\forall x)(\neg (x < 0))$

(9) $(\forall x)(0 \leq x)$

(10) $(\forall x)(\forall y)(x \leq y \iff Sx \leq Sy)$

(11) $(\forall x)(x < Sx)$

(12) $(\forall x)(\forall y)(y < Sx \iff y \leq x)$

(13) $(\forall x)(\forall y)(x \leq y \lor x \equiv y \lor y \leq x)$

Proof. Exercise! □

Proposition 7.47 (Well Founded Induction). HA proves the following:

$(\forall x)((\forall y)(y < x \Rightarrow Ay) \Rightarrow Ax) \Rightarrow (\forall x)Ax$

Proof. Exercise! □

The following is [TvD88a, Chap. 3, §3.6] (see also the Mint-Orevkov Theorem [TvD88a, Chap. 2, §3.26]).

Proposition 7.48. HA proves the following:

(1) $(\exists x)Ax \Rightarrow \neg \neg (\exists x)(Ax \land (\forall z)(z < x \Rightarrow \neg Az))$

(2) $\neg \neg [(\exists x)Ax \Rightarrow (\exists x)(Ax \land (\forall z)(z < x \Rightarrow \neg Az))]$

Proof. Exercise! □

Corollary 7.49 (Minimum Principle). PA proves the following:

$(\exists x)Ax \Rightarrow (\exists x)(Ax \land (\forall z)(z < x \Rightarrow \neg Az))$

7.3.2. The Quantifier-Free Formulae of HA

The following is essentially [Sim10, Def. I.7.8].

Definition 7.50 (The Arithmetical Hierarchy).

(1) The quantifier-free formulae of first-order arithmetic are given by the following grammar:

$A_0, B_0 ::= (a \equiv b) \mid T \mid F \mid A_0 \land B_0 \mid A_0 \lor B_0 \mid A_0 \Rightarrow B_0$
7. First-Order Arithmetic

(2) A formula is $\Pi_0^k$ (resp. $\Sigma_0^k$) if it is of the form

$$(\forall \vec{x}_1)(\exists \vec{x}_2) \cdots (Q \vec{x}_k)A_0 \quad \text{resp.} \quad (\exists \vec{x}_1)(\forall \vec{x}_2) \cdots (Q \vec{x}_k)A_0$$

where $A_0$ is quantifier-free and $Q$ is either $\forall$ or $\exists$.

Remark 7.51.

(1) Following Notation 7.27 (§7.2.5), the quantifier-free formulae of arithmetic correspond exactly to the primitive recursive predicates (since the latter are closed under Boolean operations, see e.g. [vD04, Lem. 7.1.6]).

(2) Note that the parameter $k$ in $(\forall \vec{x}_1)(\exists \vec{x}_2) \cdots (Q \vec{x}_k)A_0$ and $(\exists \vec{x}_1)(\forall \vec{x}_2) \cdots (Q \vec{x}_k)A_0$ (where $A_0$ is quantifier-free) refers to the number of quantifier alternations, and is unrelated to the lengths of the vectors $\vec{x}_i$.

Actually, thanks to (primitive recursive) pairings (Ex. 7.12, §7.2.1), it would have been (provably in HA) equivalent to define $\Pi_0^k$-formulae (resp. $\Sigma_0^k$-formulae) as the formulae of the form

$$(\forall x_1)(\exists x_2) \cdots (Qx_k)A_0 \quad \text{resp.} \quad (\exists x_1)(\forall x_2) \cdots (Qx_k)A_0$$

(with $A_0$ quantifier-free).

(3) The relevance of Def. 7.50 goes beyond first-order arithmetic (§??, see also e.g. [Sim10] as a whole). Of particular importance are the $\Sigma_0^1$-formulae and the $\Pi_0^2$-formulae, which are respectively of the form $(\exists \vec{x})A_0$ and $(\forall \vec{x})(\exists \vec{y})B_0$ with $A_0, B_0$ quantifier-free, see §7.3.3 below.

Lemma 7.52. Recall the primitive recursive functions of Ex. 7.11 (§7.2.1). In HA, we have

(1) $(a \doteq b) \iff |a - b| = 0$

(2) $(x \doteq 0 \land y \doteq 0) \iff x + y = 0$

(3) $(x \doteq 0 \lor y \doteq 0) \iff x \times y = 0$

(4) $(y = 0 \Rightarrow x \doteq 0) \iff \text{sg}(y) \times x = 0$

Corollary 7.53. Let $A_0$ be a quantifier-free formula.

(1) There is a first-order term $a$ such that HA proves

$$\vdash A_0 \iff (a \doteq 0)$$

(2) HA proves

$$\vdash A_0 \lor \neg A_0 \quad \text{and} \quad \vdash \neg\neg A_0 \Rightarrow A_0$$
7. First-Order Arithmetic

7.3.3. Relation to PA and Extraction

Perhaps the most important property of HA is that it proves the same \( \Pi^0_2 \)-formulae as PA. This result, originally due to Kreisel (see e.g. [TvD88a, Chap. 3, §10.6] or [SU06, 9.5.6]), shows in particular that HA proves the totality of the same partial recursive functions as PA (§7.2.2 and Def. 7.31, §7.2.6). In words, as alluded to in §1, when it comes to proving termination of algorithms, intuitionistic arithmetic is no weaker than classical arithmetic.

**Theorem 7.54** (Kreisel). Let \((\forall x)(\exists y)A_0\) be a closed formula with \(A_0\) quantifier-free. If PA proves \((\forall x)(\exists y)A_0\) then HA proves \((\forall x)(\exists y)A_0\).

**Corollary 7.55.** PA and HA proves the totality of the same partial recursive functions.

Theorem 7.54 is e.g. [SU06, Thm. 9.5.6] (see also [TvD88a, Chap. 3, §3.4]). We shall prove it in §7.3.4 (Thm. 7.72).

Recall that since (primitive recursive) pairing and projections are available as first-order terms of PA and HA (Ex. 7.12, §7.2.1), Thm. 7.54 extends to closed formulae of the form \((\forall x_1 \ldots x_n)(\exists y_1 \ldots y_m)A_0\). One often says that Thm. 7.54 states the “\( \Pi^0_2 \)-conservativity of PA over HA”, i.e. that PA is conservative over HA for \( \Pi^0_2 \)-sentences.

Theorem 7.54 extends to much stronger theories. We shall look at the case of Second-Order Arithmetic in §??.

Harvey Friedman ([Fri78]) has shown that Cor. 7.55 also holds for Set Theory, namely w.r.t. an intuitionistic version IZF of ZF, see e.g. [Bee85, Chap. VIII XVI] (also [TvD88b, Chap. 11, §8.11, §9.6 & §9.7]).

Theorem 7.54 is often decomposed into the two following statements:

1. For \(A_0(x, y)\) quantifier-free, if PA \(\vdash (\forall x)(\exists y)A_0(x, y)\) then HA \(\vdash (\forall x)\neg(\exists y)A_0(x, y)\).
2. HA is closed under the rule

\[
\begin{align*}
\vdash \neg\neg(\exists x)A_0 & \quad (A_0 \text{ quantifier-free}) \\
\vdash (\exists x)A_0
\end{align*}
\]

The rule in item (2) above is Markov’s Rule (see e.g. [TvD88a, Chap. 3, §3.4] or [Koh08, §14]). Beware that it has an empty context! See Rem. 7.60 below for comments on the constructivity of Markov’s Rule.

Markov’s Rule and its close (but distinct) relative Markov’s Principle

\[
(\forall x)(Ax \lor \neg Ax) \Rightarrow \neg\neg(\exists x)Ax \Rightarrow Ax
\]

(e.g. [Tro73, §1.11.5 §3.8]) have quite important roles in intuitionistic mathematics, see e.g. [TvD88a, Chap. 4, §5] or [Koh08] (as a whole).

Item (1) above can be obtained from the correctness of the negative translation \((-)^\neg\) (§6.4.4) of PA to HA.

**Theorem 7.56.** If PA proves \(A\) then HA proves \(A^\neg\).
7. First-Order Arithmetic

Theorem 7.56 easily gives Item (1) above. Indeed, from Thm 7.56 one gets that if PA proves \((\forall x)(\exists y)A_0\) with \(A_0\) quantifier-free, then HA proves \((\forall x)\neg\neg(\exists y)A_0\), from which the decidability of quantifier-free formulae in HA (Cor. 7.53, §7.3.2) gives that HA proves \((\forall x)\neg\neg(\exists y)A_0\).

Note also that Thm. 7.56 reduces the consistency of PA to the consistency of HA.

Remark 7.57. Theorem 7.56 implies that HA (as well as PA) prove all the true (closed) \(\Sigma^0_1\)-formulae. Beware that this does not hold for \(\Pi^0_1\)-formulae, because of Gödel’s Second Incompleteness Theorem 7.36 (§7.2.6).

Proof. Exercise! □

Theorem 7.56 is proven exactly as for the case of first-order logic with equality (Thm. 6.65 §6.4.4 and Thm. 6.29 §6.2.3). See [SU06, Prop. 9.5.2] and [TvD88a, Chap. 3, §3.4] for variants (in the sense of Rem. 6.32, §6.2.3). We do not further comment on this, since our way to prove Kreisel’s Theorem 7.54 in §7.3.4 will go via a generalization of the negative translation \(\neg\neg\) called Friedman’s Translation (see Prop. 7.71).

Recall from §6.2.5 that Glivenko’s Theorem 2.48 (§2.6) does not extend to the full language of first-order logic. In particular, we mentioned in Rem. 6.39 that not all formulae of the form

\[\neg\neg(\forall x_1, \ldots, x_n)(A \lor \neg A)\]

are intuitionistically provable for the reason that there are consistent intuitionistic theories which prove some formulae of the form

\[\neg(\forall x_1, \ldots, x_n)(A \lor \neg A)\]

We can now make this precise. Recall Kleene’s T predicate from Thm. 7.15 (§7.2.2).

Proposition 7.58. The extension of HA with the rule

\[\neg\forall\text{-EM}_T \vdash \neg(\forall xy)(\exists zz')T(x, y, z, z') \lor \neg(\exists zz')T(x, y, z, z')\]

induces a consistent theory, i.e. the least intuitionistic theory containing HA and the rule \((\neg\forall\text{-EM}_T)\) does not proves \(\bot\) (see Def. 6.26, §6.2.2).

In words, it is intuitionistically consistent to assume that not every computation either terminates or never halts! We shall prove Prop. 7.58 in §8.3.3 below (see also [TvD88a, Chap. 4, §3.4]). Note that Prop. 7.58 implies that there are instances of the Double Negation Shift which are not provable in HA (Rem. 6.38 and Prop. 6.37, §6.2.5).

The possibilities of extraction from proofs in HA may seem at first sight modest compared to the case of first-order logic (§6.2.6 and §6.4.6).

Theorem 7.59 (Extraction). In Heyting Arithmetic (HA),

(1) from a proof of \(\vdash A_1 \lor A_2\), with \(A_1, A_2\) closed, one can effectively compute an \(i \in \{1, 2\}\) and a proof of \(\vdash A_i\);
7. First-Order Arithmetic

(2) there is a closed formula \( A \) such that \( \vdash A \lor \neg A \) is not provable;

(3) from a proof of \( \vdash (\exists x)A \), with \( (\exists x)A \) closed, one can effectively compute a natural number \( n \in \mathbb{N} \) and a proof of \( \vdash A[n/x] \).

The conditions that the formulae are closed in item (1) and item (3) cannot be omitted. In contrast to the case of first-order logic (and recalling that disjunctions can be coded by existentials in HA (Prop. 7.43, §7.3.1)), witness extraction from proofs in arithmetic requires a proper extension of the term language. This is because the provably total functions (Def. 7.31, §7.2.6) of HA (equivalently of PA) are exactly those definable in a proper extension of the primitive recursive functions called Gödel’s System T (§8).

Note that assuming item (1), Gödel’s Incompleteness Theorems (in the form of Cor. 7.37, §7.2.6) directly give sentences \( A \) such that HA does not prove \( A \lor \neg A \) (item (2)).

We shall prove Thm. 7.59 in §8.3.4 (Cor. 8.50). We refer to [TvD88a, Chap. 3, §5.6–5.10] (see also [SU06, Prop. 9.6.6]). See [TvD88a, Chap. 3, §10.5] for historical references.

Remark 7.60 (On Markov’s Rule). Remark 7.57 immediately gives the closure of HA under the special case of Markov’s Rule

\[
\vdash \neg \neg (\exists y)A_0(y) \quad \vdash (\exists y)A_0(y)
\]

where \( A_0(y) \) has at most \( y \) free.

The constructivity of Markov’s Rule is often informally explained as follows (see e.g. [TvD88a, Chap. 4, §5.1]). Recall from Rem. 7.51 (§7.3.2) that a quantifier-free formula \( A_0(x) \) represents in the standard model (Def. 7.28, §7.2.5) a primitive recursive (and thus decidable) predicate. Consider a quantifier-free \( A_0(x,y) \) with at most \( x,y \) free. From proof in HA of

\[
\vdash \neg \neg (\exists y)A_0(x,y)
\]

we get for each \( n \in \mathbb{N} \) a proof of the closed the formula \( \neg \neg (\exists y)A_0(n,y) \), from which we know that there is some \( m \in \mathbb{N} \) such that \( A_0(n,m) \) is true (since we know it is impossible that there is none!). But (in view of Thm. 7.59.(3)), we might have no effective witness for the \( (\exists y) \). However, since \( A_0(x,y) \) is a decidable predicate, the function

\[
\begin{align*}
\mathbb{N} & \rightarrow \mathbb{N} \\
n & \mapsto \text{the least } m \in \mathbb{N} \text{ such that } A_0(n,m) \text{ is true}
\end{align*}
\]

is total recursive. We can thus witness \( (\exists y)A_0(x,y) \) by a computable function of \( x \), but in general with no further property than the mere computability of this function.

7.3.4. Friedman’s Translation

Our goal in this §7.3.4 is to prove Kreisel’s Theorem 7.54 (§7.3.3). We shall use a technique originally due to Harvey Friedman, actually following the approach of [Miq11]. We first consider a notion of parametrized negation, which then induces a parametrized negative translation. See e.g. [SU06, Lem. 9.5.5], [TvD88a, Chap. 3, §5.1 – §5.5] or [Koh08, §14] for other presentations.
Definition 7.61 (Parametrized Negation). Let $R$ be a formula of HA. The $R$-parametrized negation is

$$\neg_R A := A \Rightarrow R$$

We begin with some simple and basic properties of the parametrized negation.

Lemma 7.62. The following are provable in HA.

1. $\vdash \neg_R A \Rightarrow A \Rightarrow \neg_R B$
2. $A \vdash \neg_R \neg_R A$
3. $A \Rightarrow B \vdash \neg_R \neg_R A \Rightarrow \neg_R \neg_R B$
4. $\neg_R \neg_R \neg_R A \vdash \neg_R A$

We now define the parametrized negative translation.

Definition 7.63 (Parametrized Negative Translation). Let $R$ be a formula of HA. The parametrized negative translation of a formula $A$ of PA is the formula $A^\neg_R$ of HA defined by induction on $A$ as follows:

$$
\begin{align*}
\bot^\neg_R & := R \\
(A \land B)^\neg_R & := A^\neg_R \land B^\neg_R \\
(a \triangleq b)^\neg_R & := \neg_R(a \triangleq b) \\
(A \lor B)^\neg_R & := \neg_R(A^\neg_R \land \neg_R B^\neg_R) \\
(\forall x)A^\neg_R & := (\forall x)A^\neg_R \\
(\exists x)A^\neg_R & := \neg_R(\forall x)\neg_R A^\neg_R
\end{align*}
$$

We are going to prove important basic properties of $(-)^\neg_R$. We begin with simple facts. Note that $(\neg A)^\neg_R = \neg_R A^\neg_R$.

Lemma 7.64. The following are provable in HA, where $A$, $B$ are formulae of PA:

1. $\vdash (A \Rightarrow A \lor B)^\neg_R$
2. $\vdash (A \lor \neg A)^\neg_R$
3. $\vdash (A[a/x] \Rightarrow (\exists x)A)^\neg_R$

Proof. Exercise! \qed

We proceed with properties which require induction on formulae.

Lemma 7.65. The following are provable in HA, where $A$ is a formula of PA:
7. First-Order Arithmetic

(1) \( R \vdash A \land x \)
(2) \( \neg_{R} \neg_{R} A \land x \vdash A \land x \)

PROOF. Exercise! 

For the soundness of \( (\neg)^{\land} \) as a translation from classical to intuitionistic first-order logic, it is convenient to consider separately the following two properties.

Lemma 7.66. The following are provable in HA, where \( A, B \) and \( C \) are formulae of PA, with \( x \) not free in \( C \) nor in \( R \):

(1) \( (A \lor B)^{\land}, A^{\land} \Rightarrow C^{\land}, B^{\land} \Rightarrow C^{\land} \vdash C^{\land} \)
(2) \( ((\exists x)A)^{\land}, (\forall x)(A^{\land} \Rightarrow C^{\land}) \vdash C^{\land} \)

PROOF. Exercise! 

It is now direct to obtain the following first soundness property. If \( \Delta \) is the context \( A_{1}, \ldots, A_{m} \), then we write \( \Delta^{\land} \) for the context \( A_{1}^{\land}, \ldots, A_{m}^{\land} \).

Proposition 7.67. If \( \Delta \vdash A \) is provable in NK\(_{1}\), then \( \Delta^{\land} \vdash A^{\land} \) is provable in NJ\(_{1}\).

The proof of Prop. 7.67 is a direct extension of the corresponding property for the translation \( (\neg) \) from NK\(_{0}\) to NJ\(_{0}\) (Thm. 2.39, §2.5). Modulo Rem. 6.32 (§6.2.3), the soundness of \( (\neg) \) from NK\(_{1}\) to NJ\(_{1}\) (Thm. 6.29, §6.2.3) is essentially the instance of Prop. 7.67 with \( R := \bot \).

We now turn to the Equality Rules of Fig. 15 (§6.4.2), namely:

\[
(\neg-\text{I}) \quad \Delta \vdash a \equiv a \\
(\neg-\text{E}) \quad \Delta \vdash a \equiv b \quad \Delta \vdash A[a/x] \\
\quad \Delta \vdash A[b/x]
\]

Lemma 7.68. The following rules are admissible in NJ\(_{1}\) with equality (§6.4.2), where \( x \notin \text{FV}(R) \):

\[
\Delta \vdash \neg_{R} \neg_{R}(a \equiv a) \quad \text{and} \quad \Delta \vdash \neg_{R}(a \equiv b) \quad \Delta \vdash A^{\land}[a/x] \\
\quad \Delta \vdash A^{\land}[b/x]
\]

PROOF. Exercise! 

We thus get the extension of Prop. 7.67 to first-order logic with equality.

Corollary 7.69. If \( \Delta \vdash A \) is provable in NK\(_{1}\) with equality, then \( \Delta^{\land} \vdash A^{\land} \) is provable in NJ\(_{1}\) with equality.

The soundness of \( (\neg)^{\land} \) from NK\(_{1}\) with equality to NJ\(_{1}\) with equality (Thm. 6.65, §6.4.4) is essentially the instance of Cor. 7.69 with \( R := \bot \).

We finally turn to the axioms (i.e. non-logical rules) of PA (§7.2.4).

Lemma 7.70. If \( \Delta \vdash A \) is the conclusion of a rule of Ax\(_{\text{PR}}\) (§7.2.4), where \( \Delta, A \) are made of formulae of PA, then \( \Delta^{\land} \vdash A^{\land} \) is provable in HA.
We now have everything we need to prove that $\neg \mathbf{R}$ is provable in HA whenever $A$ is provable in PA.

**Proposition 7.71.** If $\Delta \vdash A$ is provable in PA then $\Delta \vdash \neg A$ is provable in HA.

Modulo Rem. 6.32 (§6.2.3), the soundness of the negative translation ($\neg$) from HA to PA (Thm. 7.56, §7.3.3) is Prop. 7.71 with $R := \bot$.

We can finally obtain Kreisel’s Theorem 7.54 (§7.3.3): PA is conservative over HA for $\Pi^0_2$-formulae.

**Theorem 7.72** (Kreisel’s Theorem 7.54). If $(\forall x)(\exists y)(a \equiv b)$ is provable in PA, then it is provable in HA.

The trick is to find a suitable (open) formula $R$ for $(\forall x)(\exists y)(a \equiv b)$ to be provable in HA. Since formulae of the form $A^{-}$ contain no existential quantifiers (except possibly those of $R$), it makes sense to think that $R$ should contain one.

**Proof.** Assume that $(\forall x)(\exists y)(a \equiv b)$ is provable in PA, and let $x', y'$ be fresh (distinct) variables. Let $R := (\exists y')(a'' \equiv b'')$, where $a' := a[x'/x]$, $a'' = a'[y'/y]$ and similarly for $b'$ and $b''$. By Prop. 7.71, the following is provable in HA:

$$(\forall x)(\exists y)(a \equiv b)^{-}$$

In particular, instantiating $x$ by $x'$ we get

$$\text{HA} \vdash (\exists y')(a' \equiv b')^{-}$$

and since $\neg R A \Rightarrow \neg R \neg R A$ in HA (Lem. 7.62) we obtain

$$\text{HA} \vdash \neg R (\forall y) \neg R (a' \equiv b')$$

But the latter unfolds to

$$(\forall y)((a' \equiv b') \Rightarrow R) \Rightarrow R$$

that is

$$(\forall y)((a' \equiv b') \Rightarrow (\exists y')(a'' \equiv b'')) \Rightarrow (\exists y')(a'' \equiv b'')$$

Now, we are done since

$$\text{HA} \vdash (\forall y)((a' \equiv b') \Rightarrow (\exists y')(a'' \equiv b''))$$

□
8. Gödel’s System \textbf{T}

When it comes to arithmetic, it is customary to give up looking for proof-terms in the sense of §6.3, and in particular for an exact representation of proofs as λ-terms as in Thm. 6.43. As discussed in §8.1 below, the difficulty comes from \textbf{Non Confusion (7.2.4.(1))}.

On the other hand, handling induction is not problematic, but leads to a proper extension of the simply-typed λ-calculus. The resulting calculus, known as \textbf{Gödel’s System T}, actually characterizes exactly the provably total functions of HA (and thus of PA) (§8.2), and moreover leads to a BHK interpretation of HA thanks to a notion of \textbf{Realizability (§8.3)}.

References to the literature are given within §8.2 and §8.3.

8.1. Proof-Terms for Induction

Let us look at possible proof-terms for intuitionistic arithmetic. For simplicity we consider the least intuitionistic theory of natural numbers with induction (§7.1), in which we moreover assume that disjunction is not primitive but coded using existentials as \( A \lor B \) (Prop. 7.5, §7.1).

So we might start from the following adaptation of §6.3 (and §6.4.5):

\[
 t, u ::= x \mid \lambda x.t \mid tu \mid \langle t, u \rangle \mid \pi_1 t \mid \pi_2 t \\
 | \langle \rangle \mid \text{case}_l t \{\} \\
 | \lambda x.t \mid t a \\
 | (a, t) \mid \text{let } (x, y) = t \text{ in } u \\
 | \text{eq}_I a \mid \text{eq}_E a b t u
\]

where \( a, b \) are given by the grammar

\[
 a, b ::= x \mid 0 \mid S a
\]

It follows from §6.4.5 and §6.4.2 that via \text{eq}_I and \text{eq}_E we obtain suitable proof terms for the equality axioms of Fig. 20 (§7.1). So it remains to deal with the following:

\[
 \Delta \vdash (\forall x)(S x = 0) \quad \Delta \vdash (\forall y)(S x = S y \Rightarrow x = y)
\]

\[
 \Delta \vdash A[0/x] \Rightarrow (\forall x)(A \Rightarrow A[S x/x]) \Rightarrow (\forall x)A
\]

We begin by the last one (\textit{i.e.} the \textbf{Induction Scheme 7.2.4.(2)}), which we momentarily reformulate as the rule

\[
 \Delta \vdash A[0/x] \quad \Delta \vdash (\forall x)(A \Rightarrow A[S x/x]) \\
 \frac{\Delta \vdash A[0/x] \quad \Delta \vdash (\forall x)(A \Rightarrow A[S x/x])}{\Delta \vdash (\forall x)A}
\]

Following the methodology of §4.4 and §6.3.2, consider the following possible reductions in Natural Deduction.
8. Gödel’s System T

Base Case:

\[\begin{align*}
\frac{\Delta \vdash A[0/x]}{\Delta \vdash (\forall x)(A \Rightarrow A[Sx/x])} & \quad \vdash \\
\frac{\Delta \vdash (\forall x)A}{\Delta \vdash A[0/x]} & \\
\end{align*}\]

Induction Step:

\[\begin{align*}
\frac{\Delta \vdash A[0/x]}{\Delta \vdash (\forall x)(A \Rightarrow A[Sx/x])} & \quad \vdash \\
\frac{\Delta \vdash (\forall x)A}{\Delta \vdash A[Sa/x]} & \\
\end{align*}\]

\[\begin{align*}
\frac{\Delta \vdash A[a/x] \Rightarrow A[Sa/x]}{\Delta \vdash A[Sa/x]} & \\
\end{align*}\]

This suggests to introduce a specific construction for induction at the level of proof-terms. Recall the simple type \(A^\circ\) associated to a formula \(A\) in §6.5 (on normalization of proof-terms for \(NJ_1\)). The simple types involved in the above induction rule are

\[(A[0/x])^\circ = A^\circ\]
\[(\forall x)(A \Rightarrow A[Sx/x])^\circ = \text{nat} \rightarrow (A^\circ \rightarrow A^\circ)\]
\[(\forall x)A^\circ = \text{nat} \rightarrow A^\circ\]

where we write \text{nat} for the base type \(\iota\) of §6.5. The proof-terms for induction shall be given by the \textbf{reducer} \(\text{Rec}\), with (simple) typing

\[\begin{align*}
\mathcal{E} \vdash u : T \\
\mathcal{E} \vdash v : \text{nat} \rightarrow T \rightarrow T \\
\mathcal{E} \vdash t : \text{nat} \\
\mathcal{E} \vdash \text{Rec}(u, v, t) : T
\end{align*}\]

with reductions

\[
\begin{align*}
\text{Rec}(u, v, 0) & \triangleright_\beta u \\
\text{Rec}(u, v, S\overline{t}) & \triangleright_\beta v \overline{t} \text{Rec}(u, v, t)
\end{align*}
\]

and with the following intended typing for proof-terms:

\[\begin{align*}
\mathcal{E} \vdash u : A[0/x] \\
\mathcal{E} \vdash v : (\forall x)(A \Rightarrow A[Sx/x]) \\
\mathcal{E} \vdash \lambda x.\text{Rec}(u, v, x) : (\forall x)A
\end{align*}\]
8. Gödel’s System $T$

$$
\begin{array}{c}
(0) \quad \Gamma \vdash 0 : \text{nat} \\
(\text{S}) \quad \Gamma \vdash \text{S}t : \text{nat} \\
(\text{Rec}) \quad \Gamma \vdash u : T \quad \Gamma \vdash v : \text{nat} \rightarrow T \\ 
\Gamma \vdash \text{Rec}(u,v,t) : T
\end{array}
$$

Figure 21: Additional Typing Rules for System $T$.

We now come back to the two remaining axioms above, namely:

$$
\Delta \vdash (\forall x)(Sx \neq 0) \quad \text{and} \quad \Delta \vdash (\forall x)(\forall y)(Sx \neq Sy \Rightarrow x \neq y)
$$

Still following §6.5, the simple types involved are

$$
((\forall x)(Sx \neq 0))^0 = \text{nat} \rightarrow \text{unit} \rightarrow \text{void}
$$

$$
((\forall x)(\forall y)(Sx \neq Sy \Rightarrow x \neq y))^0 = \text{nat} \rightarrow \text{nat} \rightarrow \text{unit} \rightarrow \text{unit}
$$

While it is not unreasonable to look for a proof-term for the injectivity of $S$, namely a closed $\lambda$-term of type

$$
\text{nat} \rightarrow \text{nat} \rightarrow \text{unit} \rightarrow \text{unit}
$$

there is no direct extension of proof-terms which would provide a closed $\lambda$-term of type

$$
\text{nat} \rightarrow \text{unit} \rightarrow \text{void}
$$

without making the type $\text{void}$ inhabited in the empty context, thus breaking consistency of the logical information carried-over by proof-terms (see Thm. 6.43, §6.3 and Thm. 6.55, §6.3.3).

8.2. Definition and Main Properties

This §8.2 focuses on the definition of Gödel’s System $T$ and on its main properties. Our main references are [SU06, §10] and [GLT89, §7]. Related material can be found in [TvD88b, Tro73, Koh08].

There are quite a lot of different variants of Gödel’s System $T$ considered in the literature (besides [SU06, GLT89], see e.g. [TvD88b, Tro73, Koh08]). We shall consider a version with (extended) $\lambda$-terms

$$
t, u ::= x \mid \lambda x. t \mid tu \mid \{t,u\} \mid \pi_1 t \mid \pi_2 t \mid \langle \rangle \\
\quad \mid 0 \mid \text{S}t \mid \text{Rec}(u,v,t)
$$

As for typing, we consider types over the grammar

$$
T, U ::= \text{nat} \mid U \rightarrow T \mid T \times U \mid \text{unit}
$$

The typing rules consist of the rules of Fig. 6 (§4.4.3) for the above $\lambda$-terms and types, together with the additional typing rules of Fig. 21.
Basic Rules: extension of $\triangleright_0$ (Fig. 5) with

\[
\begin{align*}
\text{Rec}(u,v,0) & \triangleright_0 u \\
\text{Rec}(u,v,St) & \triangleright_0 v \text{Rec}(u,v,t)
\end{align*}
\]

Congruence Rules: $\triangleright_\beta$ is the least relation containing $\triangleright_0$ and closed under the rules of Fig. 5 and

\[
\begin{align*}
t \triangleright_\beta t' & \implies St \triangleright_\beta St' \\
u \triangleright_\beta u' & \implies \text{Rec}(u,v,t) \triangleright_\beta \text{Rec}(u',v,t) \\
v \triangleright_\beta v' & \implies \text{Rec}(u,v,t) \triangleright_\beta \text{Rec}(u',v,t) \\
t \triangleright_\beta t' & \implies \text{Rec}(u,v,t) \triangleright_\beta \text{Rec}(u,v,t')
\end{align*}
\]

Figure 22: Additional Reduction Rules for System $\mathbf{T}$.

Notation 8.1.

(1) We often write $t : T$ for $\vdash t : T$.

(2) Similarly as for the first-order terms of arithmetic (Notation 7.2, §7.1 and Notation 7.21, §7.2.3), to each $n \in \mathbb{N}$ corresponds as numeral $n = \overbrace{S\ldots S}^{n \text{ times}} 0$.

Remark 8.2. Our choice of types (without void) implies that for each type $T$ there is a closed term $t_T$ of type $T$.

Proof. Exercise!

Concerning reduction, we consider the relation of $\beta$-reduction given by extending Fig. 5 (§4.4.3) with Fig. 22. More precisely, we first define the relation $\triangleright_0$ with the basic rules of Fig. 22 (and Fig. 5), and then let $\triangleright_\beta$ be the closure of $\triangleright_0$ under the congruence rules of Fig. 22 (and Fig. 5).

The expressive power of System $\mathbf{T}$ is quite non-trivial. We come back on this in §8.2.3.

8.2.1. Structural Properties

System $\mathbf{T}$ enjoys the same basic structural properties as the typed $\lambda$-calculi seen earlier.

Lemma 8.3 (Structural Properties).

(Weakening) If $\mathcal{E} \vdash t : T$ and $x \notin \text{dom(}\mathcal{E}\text{)}$ then $\mathcal{E}, x : U \vdash t : T$.

(Contraction) If $\mathcal{E}, x : U, y : U \vdash t : T$ then $\mathcal{E}, x : U \vdash t[x/y] : T$.

(Exchange) If $\mathcal{E}, x : U, \mathcal{E}', y : V, \mathcal{E}'' \vdash t : T$, then $\mathcal{E}, y : V, \mathcal{E}', x : U, \mathcal{E}'' \vdash t : T$.

Lemma 8.4 (Substitution). If $\mathcal{E}, x : U \vdash t : T$ and $\mathcal{E} \vdash u : U$ then $\mathcal{E} \vdash t[u/x] : T$.

Proposition 8.5 (Subject Reduction). If $\mathcal{E} \vdash t : T$ and $t \triangleright_\beta u$ then $\mathcal{E} \vdash u : T$. 

118
8. Gödel’s System $\mathbf{T}$

8.2.2. Normalization Properties

The normalization properties of System $\mathbf{T}$ are to all appearances similar to those of the typed $\lambda$-calculi seen earlier.

**Theorem 8.6** (Strong Normalization). If $E \vdash t : T$ then $t$ is strongly $\beta$-normalizing.

**Theorem 8.7** (Confluence). For each typing context $E$ and each type $T$, the relation $\triangleright_\beta$ is confluent on $|E \vdash T|$ (where $|E \vdash T|$ is defined as in Rem. 4.11, §4.2.2).

**Lemma 8.8** (Closed Typed Normal Forms). If $t$ is a closed typable term of System $\mathbf{T}$ in $\beta$-normal form, then $t$ is of one of the following forms:

$$\lambda x.u \quad \langle \rangle \quad \langle u, v \rangle \quad n$$

**Proof.** Exercise! $\square$

**Corollary 8.9.** If $\vdash t : \text{nat}$, then there is a (unique) $n \in \mathbb{N}$ such that $t \triangleright_\beta^* n$.

However, there is a crucial difference w.r.t. the $\lambda$-calculi seen earlier: the normalization of System $\mathbf{T}$ (actually already Cor. 8.9) cannot be proved in PA. We elaborate on this in §8.2.4 below. See [Tro73, §2.3.11] (see also [SU06, Cor. 10.4.11] for a related result). Just recall from §5.1 that the (strong) normalization of the simply-typed $\lambda$-calculus admits an arithmetic proof (see [SU06, §3.8] for references).

We now briefly discuss the adaptation of §5.3 to obtain Cor. 8.9. Strong Normalization (Thm. 8.6) is discussed separately in §8.2.5.

Corollary 8.9 follows from the adequacy of the following type interpretation. Given a type $T$, we write $|\vdash T|$ for the set of (closed) terms $t$ such that $\vdash t : T$.

**Definition 8.10** (Type Interpretation). For each type $T$ we define a set $\llbracket T \rrbracket \subseteq |\vdash T|$ by induction on $T$ as follows:

$$\llbracket \text{nat} \rrbracket := \{t \in |\vdash \text{nat}| : t \triangleright_\beta^* n \text{ for some } n \in \mathbb{N}\}$$
$$\llbracket U \rightarrow T \rrbracket := \{t \in |\vdash U \rightarrow T| : (\forall u \in |\llbracket U \rrbracket)(tu \in |\llbracket T \rrbracket)\}$$
$$\llbracket T \times U \rrbracket := \{t \in |\vdash T \times U| : \pi_1 t \in |\llbracket T \rrbracket \text{ and } \pi_2 t \in |\llbracket U \rrbracket\}$$

**Lemma 8.11.** If $t \in |\llbracket T \rrbracket|$ and $u \triangleright_\beta^* t$ with $u : T$, then $u \in |\llbracket T \rrbracket|$.

Note that

- $0 \in |\llbracket \text{nat} \rrbracket|$;
- $St \in |\llbracket \text{nat} \rrbracket|$ for all $t \in |\llbracket \text{nat} \rrbracket|$;
- and thus $n \in |\llbracket \text{nat} \rrbracket|$ for all $n \in \mathbb{N}$.

The following seemingly obvious property is essentially the cause of the unprovability of Cor. 8.9 in PA.

**Lemma 8.12.** Assume $u \in |\llbracket T \rrbracket|$ and $v \in |\llbracket \text{nat} \rightarrow T \rightarrow T \rrbracket|$. Then:
8. Gödel’s System T

(1) \( \text{Rec}(u, v, n) \in \texttt{[}[T]\texttt{]} \) for all \( n \in \mathbb{N} \).

(2) \( \text{Rec}(u, v, t) \in \texttt{[}[T]\texttt{]} \) for all \( t \in \texttt{[}[\text{nat}]\texttt{]} \).

The adequacy of the type interpretation of Def. 8.10 is then an easy adaptation of §5.3.2 and §5.3.3.

Remark 8.13. Similarly as in §5.3.1, Cor. 8.9 already holds for a weak variant of \( \triangleright_\beta \), namely the (deterministic) relation \( \triangleright_T \) given by \( E[t] \triangleright_T E[u] \) if \( t \triangleright_0 u \) (where \( \triangleright_0 \) is given by Fig. 22) and \( E[ ] \) is a context on the grammar

\[
E[ ], F[ ] ::= \[ \] \mid E[ ] t \mid \pi_1 E[ ] \mid \pi_2 E[ ] \mid S E[ ] \mid \text{Rec}(u, v, F[ ])
\]

where \( F[ ] \) is not of the form \( SE[ ] \).

Proof. Exercise!

8.2.3. Expressiveness and Representation

Maybe the most important property of Gödel’s System T is that it exactly characterizes the provably total functions of HA (equivalently of PA).

We begin with some easy consequences of Cor. 8.9 (§8.2.2).

Notation 8.14 (Representation in System T).

(1) Given \( t : \text{nat} \), we write \( [t] \in \mathbb{N} \) for the unique natural number such that \( t \triangleright^*_\beta [t] \).

(2) Given \( t : \text{nat}^k \to \text{nat} \), we write \( [t] : \mathbb{N}^k \to \mathbb{N} \) for the function

\[
(\ldots \times \mathbb{N} \to \mathbb{N}
(\ldots n_k) \mapsto [t(n_1 \ldots n_k)]
\]

(3) We say that a function \( f : \mathbb{N}^k \to \mathbb{N} \) is represented by a term \( t : \text{nat}^k \to \text{nat} \) if \( f = [t] \).

All primitive recursive functions (§7.2.1) are representable in System T.

Exercise 8.15. Give a System T term \( \text{add} : \text{nat} \times \text{nat} \to \text{nat} \) which represents addition on natural numbers.

Proof. Exercise!

Proposition 8.16. If \( f : \mathbb{N}^k \to \mathbb{N} \) is primitive recursive, then there is a System T term \( t : \text{nat}^k \to \text{nat} \) which represents \( f \).

Proof. Exercise!

However, System T represents more than the primitive recursive functions. We refer to [SU06, §10] and [GLT89, §7].
Exercise 8.17 (Ackermann Function). A typical function which is representable in System T but not primitive recursive is the well-known Ackermann function. We follow the presentation of [SU06, Ex. 10.3, 10.5 & 10.6], but see also [GLT89, §7.3.2].

Consider the function \( f : n \mapsto f_n(n) \), where the functions \( (f_k : \mathbb{N} \to \mathbb{N})_{k \in \mathbb{N}} \) are defined as
\[
\begin{align*}
 f_0(n) &= n + 1 \\
 f_{k+1}(n) &= f_k^n(n) \quad (f_k \text{ applied } n \text{ times to } n)
\end{align*}
\]
The function \( f : n \mapsto f_n(n) \) is not primitive recursive. Show that it is representable in System T.

**Proof.** Exercise!

The main extraction result relating HA and System T is the following.

**Theorem 8.18.** From a proof of \( \vdash (\forall x_1 \ldots x_k)(\exists y)A(x_1, \ldots, x_k, y) \) in HA (where \( A \) has free variables among \( x_1, \ldots, x_k, y \)), one can effectively compute a System T term \( t : \mathbb{N}^k \to \mathbb{N} \) such that for all \( n_1, \ldots, n_k \in \mathbb{N} \), the formula \( A(n_1, \ldots, n_k, [t(n_1, \ldots, n_k)]) \) is provable in HA.

**Corollary 8.19.** From a proof of \( (\forall x)(\exists y)P(x, y) \) in HA (where \( P(x, y) \) is a primitive recursive predicate), one can effectively compute a System T term \( t \) such that \( \vdash t : \mathbb{N} \to \mathbb{N} \) and \( P(n, [t(n)]) \) for all \( n \in \mathbb{N} \).

Corollary 8.19 of course extends to PA by Kreisel’s Theorem 7.54 (§7.3.3). We shall prove Thm. 8.18 and Cor. 8.19 in §8.3 (Cor. 8.51 and Cor. 8.37 respectively) using a notation of Realizability.

Corollary 8.19 implies that the provably total functions of PA and HA (Def. 7.31, §7.2.6) are all representable in System T. The converse is actually true, as stated in the following.

**Theorem 8.20 (Representation).** The following are equivalent for a partial recursive function \( f : \mathbb{N} \to \mathbb{N} \):

(i) \( f \) is provably total in PA;

(ii) \( f \) is provably total in HA;

(iii) \( f = [t] \) for some term \( t \) such that \( \vdash t : \mathbb{N} \to \mathbb{N} \).

Theorem 8.20 is essentially [Tro73, Thm. 3.4.29]. It relies on tedious manipulations of Gödel’s numbers representing System T terms in HA. We briefly comment on this in §8.2.4 below, but we refer to e.g. [Tro73, Thm. 3.4.29] for details (and to [GLT89, §7.4.2] for an informal account).

Let us finally mention that products types \( ((-) \times (-), \text{unit}) \) are not required for Cor. 8.19 and Thm. 8.20 (see Rem. 8.38, §8.3).
8. Gödel’s System T

8.2.4. Arithmetization

This §8.2.4 overviews aspects of Gödel’s System T related to its representation in first-order arithmetic via suitable Gödel’s numbers. We use notations for these similar to those of §7.2.2 and §7.2.6 (see also §7.2.7). However, we shall not define the codings in full detail, and only loosely follow the approach of [vdD04, §7.6] (on the representation of PA0 in PA0). We target two results:

1) Proposition 8.23, namely the unprovability in PA of the Normalization of System T (in the form of Cor. 8.9, §8.2.2), which is essentially a diagonalization argument based on extraction for Π02-formulae (Cor. 8.19, §8.2.3) and using suitable Gödel numbers. (See [Tro73, §2.3.11], see also [SU06, Cor. 10.4.11] for a related result.)

2) A sketch of the remaining part of Thm. 8.20 (§8.2.3), namely that the functions representable in System T are provable total in PA [Tro73, Thm. 3.4.29].

We consider a typed syntax for System T. First we assume for each type T a countably infinite set of variables XT = {xT, yT, zT, etc}. The typed terms are then given by the following grammar, where types are indicated as superscripts:

\[
t^T, u^U ::= x^T | (λx^U.t^T) \rightarrow ^T | (t^U \rightarrow ^T u^U)^T \\
| (\langle t^T, u^U \rangle)^{T \times U} | (\pi_1^{T \times U})^T | (\pi_2^{T \times U})^U \\
| 0^n | (\text{S}t^n)^{n} | (\text{Rec}(u^T, v^n \rightarrow ^T t, t^n))^T
\]

Notation 8.21. When possible, we drop the type superscript and write t for t^T. We also often write t : T (or ⊢ t : T) for t^T.

Assumption 8.22. We assume given

(a) for each term t a Gödel number ⊢ t ∈ N, for each type T a Gödel number ⊢ □ T ∈ N, and

(b) primitive recursive functions app(x, y), succ(x), num(x) and

(c) primitive recursive predicates Typing(x, y, z), Norm(x, y, z)

such that

(i) app(⊢ t, ⊢ u) = ⊢ tu, succ(⊢ t) = ⊢ S\text{t}, num(n) = ⊢ n^n, and

(ii) Typing(⊢ t, ⊢ □ T) if and only if ⊢ t : T, and

(iii) Norm(⊢ t, n, k) if and only if t ⊢ k \in N.

Following e.g. [vdD04, §7.6], we can assume that Gödel’s numbers for types consist of pairs ⟨x\text{c}, x\text{d}⟩ where x\text{c} ranges among predefined integer values z\text{c} for each constructor \text{c} of the syntax of types of System T, and where x\text{d} is a tuple whose length is the arity of the corresponding constructor and whose components are the code the corresponding sub-expressions. For terms, we assume a similar coding but this times as triples ⟨x\text{e}, x\text{f}, x\text{g}⟩ to

122
where \(x_1\) is ranges over predefined codes \(c\) for term constructors \(c\), \(x_2\) is a tuple whose components are the sub-terms and where \(x_3\) is the type. For instance:

\[
\begin{align*}
\langle \text{nat} \rangle &= \langle \sharp \text{nat}, (\rangle \rangle \\
\langle U \rightarrow T \rangle &= \langle \sharp \rightarrow, (\langle U \rangle, \langle T \rangle) \rangle \\
\langle 0 \rangle &= \langle \sharp \text{0}, (\rangle \rangle \\
\langle St \rangle &= \langle \sharp \text{S}, (\langle t \rangle), \langle \text{nat} \rangle \rangle \\
\langle (tu)T \rangle &= \langle \sharp \text{@}, (\langle t \rangle, \langle u \rangle), \langle T \rangle) \rangle
\end{align*}
\]

Moreover the primitives recursive functions app, succ and num are such that

\[
\begin{align*}
succ(x) &= \langle \sharp \text{S}, (x), \langle \text{nat} \rangle \rangle \\
um(0) &= \langle \sharp \text{0}, (\rangle \rangle \\
um(S(x)) &= \langle \sharp \text{S}, (\text{num}(x)), \langle \text{nat} \rangle \rangle \\
app(x, y) &= \langle \sharp \text{@}, (x, y), (\pi_2 \circ \pi_2 \circ \pi_3)(x) \rangle
\end{align*}
\]

The predicate Typing\((x, y)\) can be defined from the function typeof\((x)\) with

\[
\text{typeof}(x) = \pi_3(x)
\]

As for Norm\((x, y, z)\), we can rely on Rem. 8.13 (§8.2.2) and instead of \(\triangleright_{\beta}\) consider the deterministic relation \(\triangleright_{\tau}\) represented as a primitive recursive function.

**Proposition 8.23.** PA does not prove \(\forall x(\exists z)(\text{Typing}(x, \langle \text{nat} \rangle) \Rightarrow \text{Norm}(x, \pi_1 z, \pi_2 z))\).

**Proof.** Assume toward a contradiction that PA proves the formula. Consider the primitive recursive relation

\[
P(x, a, b, z) := \text{Norm(succ(app(x, num(a)))), b, z)}
\]

It follows from our Assumption 8.22 that

\[
P(\langle u \rangle, n, m, k) \text{ iff Norm(succ(app(\langle u \rangle, num(n))), m, k) iff Norm(succ(app(\langle u \rangle, \langle n \rangle)), m, k)}
\]

Our assumptions on Gödel numbers easily implies that PA proves the following

\[
\vdash \text{Typing}(\text{num}(x), \langle \text{nat} \rangle) \quad \vdash \text{Typing}(\text{app}(x, \text{num}(x)), \langle \text{nat} \rangle)
\]

It follows that PA proves

\[
(\forall x)(\exists z)(\text{Typing}(x, \langle \text{nat} \rightarrow \text{nat} \rangle) \Rightarrow P(x, x, \pi_1 z, \pi_2 z))
\]

123


Since the above relation is primitive recursive (as primitive recursive relations are closed under Boolean operations, see e.g. [vD04, Lem. 7.1.6]), it follows from Cor. 8.19 (§8.2.3) and from our Assumption 8.22 that there is a term \( t : \text{nat} \to \text{nat} \) such that for all \( u : \text{nat} \to \text{nat} \) and all \( n \in \mathbb{N} \), we have \( S^k(u \overline{n}) \triangleright^k m \) for some \( k \in \mathbb{N} \), where \( m = [t \overline{u}] \). But this implies that \( S^k(t \overline{u}) \triangleright^k [t \overline{t}] \) for some \( k \in \mathbb{N} \), a contradiction since \( S^k(t \overline{u}) \triangleright^k S[t \overline{t}] \).

Extending Assumption 8.22 where necessary, we finally note here that we can define for each type \( T \) a formula \( \text{Norm}^J_T \) which represents in \( \text{PA} \) the set \( \text{Def. 8.10, §8.2.2} \).

Typical clauses are

\[
\text{Norm}^J_{\text{nat}}(x) := \text{Typing}(x, \overline{\text{nat}}) \land (\exists y)(\exists z)\text{Norm}(x, y, z)
\]

\[
\text{Norm}^J_{U \to T}(x) := \text{Typing}(x, \overline{U \to T})
\]

\[
\land (\forall y)(\text{Norm}^J_U(y) \Rightarrow \text{Norm}^J_T(\text{app}(x, y)))
\]

Note that (under Assumption 8.22) \( \text{PA} \) proves

\[
\text{Norm}^J_{\text{nat} \to \text{nat}}(x) \vdash (\forall y)(\exists z)(\exists w)\text{Norm}(\text{app}(x, \text{num}(y)), z, w)
\]

We can similarly write clauses expressing a form of higher-type computability. Possible clauses are

\[
\text{Comput}^J_{\text{nat}}(x) := \top
\]

\[
\text{Comput}^J_{U \to T}(x) := (\forall y)\left(\text{Comput}^J_U(y) \Rightarrow (\exists z)(\exists w)\left(\text{T}(x, y, z, w) \land \text{Comput}^J_T(z)\right)\right)
\]

where \( \text{T} \) is Kleene’s predicate (Thm. 7.15, 7.2.2). Note that \( \text{Comput}^J_{\text{nat} \to \text{nat}}(x) \) amounts to

\[
(\forall y)(\exists z)(\exists w)\text{T}(x, y, z, w)
\]

The missing part of the Representation Theorem. 8.20 (§8.2.3) is obtained essentially by showing that for every \( t : \text{nat} \to \text{nat} \), there is a partial recursive function \( f : \mathbb{N} \to \mathbb{N} \) such that \([t] = f\) and such that \( \text{PA} \) proves \( \text{Comput}^J_{\text{nat} \to \text{nat}}(e_f) \). See [Tro73, Thm. 3.4.29] for details.

8.2.5. Strong Normalization

We briefly discuss here the adaptation of §5.5 to the strong normalization of (typed) System \( T \) terms (Thm. 8.6, §8.2.2).

We consider the following elimination contexts:

\[
E[\ ], F[\ ] \in \text{Elim} := [\ ] \mid E[\ ] t \mid \pi_1 E[\ ] \mid \pi_2 E[\ ]
\]

\[
\mid \text{Rec}(u, v, E[\ ])
\]

where (in contrast with Rem. 8.13, §8.2.2), we do not allow elimination contexts of the form \( S E[\ ] \).

We consider the notion Weak Head Reduction \( \triangleright_{\text{wh}} \) given by the direct application of Def. 5.4 (§5.3.1) to the above elimination contexts.

Recall the notion of tuple reduction of Notation 5.25 (§5.5.2). The analogue of the Weak Standardization Lemma 5.26 (§5.5.2) is the following:
Lemma 8.24 (Weak Standardization). Let $E[ ] \in \text{Elim}$.

1. If $E[(\lambda x.t)u] \beta v$, then either $v = E[t/u] \in S\mathcal{N}$ or $v$ is of the form $E'[(\lambda x.t')u']$ with $(E[ ], t, u) \beta (E'[ ], t', u')$.

2. Let $i \in \{1, 2\}$. If $E[\pi_i(t_1, t_2)] \beta v$, then either $v = E[t_i]$ or $v$ is of the form $E'[(\pi_i(t_1', t_2'))]$ with $(E[ ], t_1, t_2) \beta (E'[ ], t_1', t_2')$.

3. If $E[\text{Rec}(u, v, 0)] \beta w$, then either $w = E[u]$ or $w$ is of the form $E'[\text{Rec}(u', v', 0)]$ where $(E[ ], u, v) \beta (E'[ ], u', v')$.

4. If $E[\text{Rec}(u, v, s t)] \beta w$, then either $w = E[v t \text{Rec}(u, v, t)]$ or $w$ is of the form $E'[\text{Rec}(u', v', s t')]$ where $(E[ ], u, v, t) \beta (E'[ ], u', v', t')$.

**Proof.** Exercise!

The Weak Head Expansion Lemma 5.27 is then adapted to the following.

Lemma 8.25 (Weak Head Expansion). Let $E[ ] \in \text{Elim}$.

1. If $E[t/u] \in S\mathcal{N}$ and $u \in S\mathcal{N}$ then $E[(\lambda x.t)u] \in S\mathcal{N}$.

2. Let $i \in \{1, 2\}$. If $E[t_i] \in S\mathcal{N}$ and $t_{3-i} \in S\mathcal{N}$ then $E[\pi_i(t_1, t_2)] \in S\mathcal{N}$.

3. If $E[u] \in S\mathcal{N}$ and $v \in S\mathcal{N}$ then $E[\text{Rec}(u, v, 0)] \in S\mathcal{N}$.

4. If $E[v t \text{Rec}(u, v, t)] \in S\mathcal{N}$ then $E[\text{Rec}(u, v, \text{Rec}(u, v, s t))] \in S\mathcal{N}$.

**Proof.** Exercise!

This leads to the following notion of **Saturated Set** (Def. 5.28, §5.5.3).

Definition 8.26 (Saturated Sets). The set $\text{SAT}$ of saturated sets is the set of all $A \subseteq S\mathcal{N}$ such that

1. $E[x] \in A$ whenever $E[ ] \in \text{Elim} \cap S\mathcal{N}$, and
2. $E[(\lambda x.t)u] \in A$ whenever $u \in S\mathcal{N}$ and $E[t/u] \in A$, and
3. for all $i \in \{1, 2\}$, $E[\pi_i(t_1, t_2)] \in A$ whenever $t_{3-i} \in S\mathcal{N}$ and $E[t_i] \in A$, and
4. $E[\text{Rec}(u, v, 0)] \in A$ whenever $v \in S\mathcal{N}$ and $E[u] \in A$, and
5. $E[\text{Rec}(u, v, s t)] \in A$ whenever $E[v t \text{Rec}(u, v, t)] \in A$.

**Lemma 8.27.** Saturated sets are stable under weak head expansion: given $A \in \text{SAT}$ and $t \in A$, if $u \triangleright_{wh} t$ with $u \in S\mathcal{N}$ then $u \in A$.

**Proof.** Exercise!

**Lemma 8.28.** The set $\text{SAT}$ is a complete lattice w.r.t. inclusion, whose top element is $\top := S\mathcal{N}$ and whose least element is $\bot := \{t \in S\mathcal{N} \mid (\exists E[ ])(t \triangleright_{wh} E[x])\}$.
8. Gödel’s System T

We have the obvious analogue of Lem. 5.30 (§5.5.3).

**Lemma 8.29.** Let $A, B \in \text{SAT}$. Then

$$A \rightarrow B, A \sqsubset B \in \text{SAT}$$

**Proof.** Exercise! □

The interpretation of types shall follow §5 for $(-) \rightarrow (-)$ and $(-) \times (-)$. The type nat requires a specific fixpoint.

**Definition 8.30.** We let $\mathcal{N}$ be the least fixpoint (in the complete lattice $\text{SAT}$) of the (monotone) function

$$\text{SAT} \rightarrow \text{SAT}$$

$$X \mapsto \bot \cup \{t \in \mathcal{N} \mid t \triangleright^* 0\} \cup \{t \in \mathcal{N} \mid (\exists u \in X)(t \triangleright^* S u)\}$$

It is clear that $0 \in \mathcal{N}$ and that $St \in \mathcal{N}$ whenever $t \in \mathcal{N}$. Moreover,

**Lemma 8.31.** Let $A \in \text{SAT}$. Assume $u \in A$, $v \in (\mathcal{N} \rightarrow A \rightarrow A)$ and $t \in \mathcal{N}$. Then $\text{Rec}(u, v, t) \in A$.

**Proof.** Exercise! □

We thus get an adequate type interpretations with

$$\text{nat} := \mathcal{N} \quad [U \rightarrow T] := [U] \rightarrow [T] \quad [T \times U] := [T] \sqsubset [U]$$

Strong normalization of the (typed) terms of System T (Thm. 8.6, §8.2.2) immediately follows.

### 8.3. Modified Realizability

Realizability is a technique introduced by S. C. Kleene as a formal counterpart to the informal Brouwer-Heyting-Kolmogorov (BHK) of intuitionistic arithmetic. Let us recapitulate the clauses of the BHK interpretation given in §4.1 and §6.3, but adapted to arithmetic (where the term “proof” should be understood as some informal notion of “witness of evidence”):

- there is no “proof” of $\bot$;
- a “proof” of $A_1 \land A_2$ is a pair of a “proof” of $A_1$ and a “proof” of $A_2$;
- a “proof” of $A_1 \lor A_2$ is a (dependent) pair of an $i \in \{1, 2\}$ and a “proof” of $A_i$;
- a “proof” of $A \rightarrow B$ is a “function” taking a “proof” of $A$ to a “proof” of $B$;
- a “proof” of $(\forall x)A$ is a “function” which takes a natural number $n \in \mathbb{N}$ to a “proof” of $A[n/x]$;
8. Gödel’s System T

\[(a \equiv b)^\circ := \text{unit} \]
\[\top^\circ := \text{unit} \]
\[\bot^\circ := \text{unit} \]
\[(A \Rightarrow B)^\circ := A^\circ \rightarrow B^\circ \]
\[(A \land B)^\circ := A^\circ \times B^\circ \]
\[(\forall x A)^\circ := \text{nat} \rightarrow A^\circ \]
\[(\exists x A)^\circ := \text{nat} \times A^\circ \]

Figure 23: Erasure Map from (Open) Formulae to Types.

- a “proof” of \((\exists x) A\) is a (dependent) pair of a natural number \(n \in \mathbb{N}\) and a “proof” of \(A[n/x]\).

Kleene’s original formulation of realizability was based on partial recursive functions, and interpreted intuitionistic arithmetic (which in particular allowed for the extraction of computable witnessing function from proofs of \(\forall\exists\)-formulae).

Nowadays, realizability exists in various forms. Besides Kleene’s original version (for which we refer to [TvD88a, Chap. 4, §4], also [SU06, §9.6], and [Bee85, §VIII]), the general methodology of realizability has been adapted to different computational models, e.g. computable functions on streams of natural numbers (see e.g. [Tro73, §3] or [KV65]), \(\lambda\)-calculi (or Combinatory Logics) either typed (e.g. [Tro73, §3.4] or [Koh08, §5]) or untyped (see e.g. [Kri93, §9]), as well as to different logics (we shall see the case of Second-Order Arithmetic in §?? below). One of the most important development is Krivine’s work on realizability for classical logic [Kri09], which actually goes as far as ZF set theory [Kri01].

In any case, realizability is a very interesting computation-based tool to generate logical theories. We shall see in §8.3.3 below an example of a coherent intuitionistic theory which validates non-classical principles. But we also (again) refer to Krivine’s work on models of ZF [Kri12].

In this §8.3, we concentrate on a simple variant of Kleene’s Realizability, known as Kreisel’s Modified Realizability, and which is based on System T. Besides [SU06, §10.4] (whose presentation largely differs from ours), we refer to [Koh08, §5] and [Tro73, §3.4] (which consider an internalized notion of (typed) realizability, based on Combinatory Logic).

The basic idea is a refinement of the above BHK interpretation, where a “proof” is taken to be a (closed) typed term of System T. We thus first associate to each (possibly open) formula \(A\) a type \(A^\circ\). We begin by only considering formulae of HA without disjunction (recall from §7.1 and Prop. 7.43, §7.3.1 that this is not a restriction in terms of expressiveness). The clauses for \(A^\circ\) are given in Fig. 23. They should be strongly reminiscent from those of Fig. 17 (for the normalization of the proof-terms of NJ\(_1\), §6.5). But beware that we now take

\[\bot^\circ = \text{unit} \]
8. Gödel’s System T

\[ t \vdash (a = b) \iff [a] = [b] \]
\[ t \not\vdash \top \]
\[ t \vdash A \Rightarrow B \iff \text{for all } u \vdash A, \text{ we have } tu \vdash B \]
\[ t \vdash A \land B \iff \pi_1t \vdash A \text{ and } \pi_2t \vdash B \]
\[ t \vdash (\forall x)A \iff \text{for all } n \in \mathbb{N}, t_n \vdash A[n/x] \]
\[ t \vdash (\exists x)A \iff \text{there exists } n \in \mathbb{N} \text{ such that } \pi_1t \triangleright^* n \text{ and } \pi_2t \vdash A[n/x] \]

Figure 24: The Realizability Relation \( t \vdash A \) (where \( t, A \) are closed and \( \vdash t : A^\circ \)).

**Definition 8.32** (Modified Realizability). The realizability relation \( t \vdash A \), where \( A \) is a closed formula and \( t : A^\circ \), is defined by induction on \( A \) with the clauses of Fig. 24. We say that \( t \) realizes \( A \) when \( t \vdash A \) and that \( A \) is realized when \( t \vdash A \) for some \( t \).

**Example 8.33** (Non-Confusion). Taking \( \bot^\circ = \text{unit} \) solves the problem raised in §8.1 with the Non-Confusion axiom 7.2.4.(1)

\[ (\forall x)(Sx = 0) \]

Indeed, we have

\[ \lambda x.\lambda y.\langle \rangle \vdash (\forall x)((Sx = 0) \Rightarrow \bot) \]

First, note that

\[ \lambda x.\lambda y.\langle \rangle : ((\forall x)((Sx = 0) \Rightarrow \bot))^\circ = \text{nat} \rightarrow \text{unit} \rightarrow \text{unit} \]

Second, we have

\[ \lambda x.\lambda y.\langle \rangle \vdash (\forall x)((Sx = 0) \Rightarrow \bot) \]
\[ \text{iff for all } n \in \mathbb{N}, (\lambda x.\lambda y.\langle \rangle)_n \vdash ((Sn = 0) \Rightarrow \bot) \]
\[ \text{iff for all } n \in \mathbb{N}, \text{ for all } u \vdash (Sn = 0), (\lambda x.\lambda y.\langle \rangle)_n u \vdash \bot \]

But given \( n \in \mathbb{N} \), we have \( (\lambda x.\lambda y.\langle \rangle)_n u \vdash \bot \) for all \( u : \text{unit} \) such that \( u \vdash Sn = 0 \), since there is no \( u : \text{unit} \) such that \( u \vdash Sn = 0 \) (as \( \|Su\| = n + 1 \neq 0 = \|0\| \)).

We now turn to a couple of customary properties of (modified) realizability.

**Lemma 8.34.** Let \( a, b \) be closed first-order terms such that \([a] = [b] \). Then \( t \vdash A[a/x] \) if and only if \( t \vdash A[b/x] \).

**Lemma 8.35.** If \( t \vdash A \) and \( u \triangleright^* t \) with \( u : A^\circ \) then \( u \vdash A \).

The main result on (modified) realizability is that intuitionistically provable formulae are realized.

**Theorem 8.36** (Adequacy). From a proof of \( \vdash A \) in HA (with \( A \) closed), one can effectively compute a term \( t \) of System T such that \( t \vdash A \).
8. Gödel’s System T

The extraction of witnessing functions from proofs of $\Pi^0_2$-formulae (Cor. 8.19, §8.2.3), is a direct consequence of the Adequacy Theorem 8.36.

Corollary 8.37 (Cor. 8.19). From a proof of $(\forall x)(\exists y)P(x,y)$ in HA (where $P(x,y)$ is a primitive recursive predicate), one can effectively compute a System T term $t$ such that $\vdash t : \text{nat} \rightarrow \text{nat}$ and $P(n,[tn])$ for all $n\in \mathbb{N}$.

Proof. By Def. 7.13 (§7.2.1), there is a first-order term $p(x,y)$ such that HA proves $(\forall x)(\exists y)p(x,y) \equiv 1$. By the Adequacy Theorem 8.36, there is a term $\vdash u : \text{nat} \rightarrow \text{nat} \times \text{unit}$ such that for all $n\in \mathbb{N}$, we have $\pi_2(un) \vdash p(n,[\pi_1(un)]) \equiv 1$. Let $t := \lambda x.\pi_1(ux)$. By definition of realizability for equalities, we get that $p(n,[tn]) = 1$ for all $n\in \mathbb{N}$, and the result follows by Lem. 8.35.

Remark 8.38. Products types $(-)\times(-)$, unit are actually not required for Cor. 8.37. This can be seen via an appropriate notion of (modified) realizability, as presented in e.g. [Koh08, §5].

The remaining of this §8.3 is organized as follows. First, we prove Thm. 8.36 in §8.3.1. An extension of modified realizability which handles (primitive) disjunctions is discussed in §8.3.2. Note that Thm. 8.36 means that (modified) realizability is compatible with intuitionistic deduction. In other words, the set of realized formulae is a (consistent) intuitionistic theory. We elaborate on this in §8.3.3. Finally, we discuss in §8.3.4 a variation on (modified) realizability which gives the extraction properties of HA (Thm. 7.59, §7.3.3 and Thm. 8.18, §8.2.3).

8.3.1. Proof of Adequacy

The inductive invariant of the Adequacy Theorem 8.36 is the following, where we use a vectorial notation for simultaneous substitution (§5.2), e.g. if $\vec{y} = y_1, \ldots, y_n$ and $\vec{u} = u_1, \ldots, u_n$, then $t[\vec{u}/\vec{y}]$ stands for $t[u_1/y_1, \ldots, u_n/y_n]$.

Proposition 8.39. Assume that $A_1, \ldots, A_n, A$ have free (first-order) variables among $x_1, \ldots, x_k$. From a proof of $A_1, \ldots, A_n \vdash A$ in HA, one can effectively compute a term $t$ of System T such that

(i) $x_1 : \text{nat}, \ldots, x_k : \text{nat}, y_1 : A_1^\circ, \ldots, y_n : A_n^\circ \vdash t : A^\circ$, and

(ii) for all $m_1, \ldots, m_k \in \mathbb{N}$ and all $u_1 \vdash A_1[m_/x_1], \ldots, u_n \vdash A_n[m_/x_n]$, we have $t[m_/x, \vec{u}/\vec{y}] \vdash A[m_/x]$.

Notation 8.40. We write $y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A$ when $t$ satisfies conditions (i) and (ii) of Prop. 8.39. Beware that in contrast with Def. 8.32, this assumes neither $t$ nor $A_1, \ldots, A_n, A$ to be closed.

Proposition 8.39 is proven by induction on derivations. We begin with the case of NJ1 (without disjunction).

Lemma 8.41. From a proof of $A_1, \ldots, A_n \vdash A$ in NJ1 (without disjunction), one can effectively compute a term $t$ of System T such that $y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A$.
8. Gödel’s System $\mathbf{T}$

**Proof.** By induction on $\Delta \vdash A$, where $\Delta$ is the context $A_1, \ldots, A_n$.

**Case of**

$(\text{Ax}) \quad \frac{\Delta \vdash A_i}{\Delta \vdash A_i}$

We are done by taking for $t$ the typed term

$x_1 : \text{nat}, \ldots, x_k : \text{nat}, y_1 : A^\circ_1, \ldots, y_n : A^\circ_n \vdash y_i : A^\circ_i$

**Case of**

$(\top-I) \quad \frac{}{\Delta \vdash \top}$

We are done by taking for $t$ the typed term

$x_1 : \text{nat}, \ldots, x_k : \text{nat}, y_1 : A^\circ_1, \ldots, y_n : A^\circ_n \vdash \langle \rangle : \top^\circ$

**Case of**

$(\perp-E) \quad \frac{\Delta \vdash \bot \quad \Delta \vdash A}{\Delta \vdash A}$

The induction hypothesis gives a term $t$ such that $y_1 : A_1, \ldots, y_n : A_n \vdash t \parallel \bot$. By Rem. 8.2 ($\S 8.2$) we get a (closed) term $t_A$ of type $A^\circ$. We claim that $y_1 : A_1, \ldots, y_n : A_n \vdash t_A \parallel A$.

Take $m_1, \ldots, m_k \in \mathbb{N}$ and $u_1 \parallel A_1[m/x], \ldots, u_n \parallel A_n[m/x]$. By assumption we have $t[m/x, u/y] \parallel \bot$, a contradiction, from which we can get $t_A \parallel A[m/x]$.

**Case of**

$(\Rightarrow-I) \quad \frac{\Delta, A \vdash B \quad \Delta \vdash A \Rightarrow B}{\Delta \vdash B}$

The induction hypothesis gives a term $t$ such that $y_1 : A_1, \ldots, y_n : A_n, y : A \vdash t \parallel B$. We claim that $y_1 : A_1, \ldots, y_n : A_n \vdash \lambda x. t \parallel A \Rightarrow B$.

Let $m_1, \ldots, m_k \in \mathbb{N}$ and $u_1 \parallel A_1[m/x], \ldots, u_n \parallel A_n[m/x]$. We have to show $(\lambda y. t)[m/x, u/y] \parallel A[m/x] \Rightarrow B[m/x]$. So let $u \parallel A[m/x]$. By assumption we have $t[m/x, u/y] \parallel B[m/x]$ and we conclude by Lem. 8.35.

**Case of**

$(\Rightarrow-E) \quad \frac{\Delta \vdash A \Rightarrow B \quad \Delta \vdash A}{\Delta \vdash B}$

By induction hypothesis, we get $y_1 : A_1, \ldots, y_n : A_n \vdash t \parallel A \Rightarrow B$ and $y_1 : A_1, \ldots, y_n : A_n \vdash u \parallel A$. We claim that $y_1 : A_1, \ldots, y_n : A_n \vdash t u \parallel B$.

Given $m_1, \ldots, m_k \in \mathbb{N}$ and $u_1 \parallel A_1[m/x], \ldots, u_n \parallel A_n[m/x]$, we have $(t u)[m/x, u/y] = (t[m/x, u/y])u[m/x, u/y]$, and we are done since by assumption $t[m/x, u/y] \parallel A[m/x]$ and $u[m/x, u/y] \parallel A[m/x]$. 

130
8. Gödel’s System T

Case of
\[ (\land \mathbf{I}) \quad \Delta \vdash A \quad \Delta \vdash B \quad \frac{}{\Delta \vdash A \land B} \]

By induction hypothesis, we get \( y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A \) and \( y_1 : A_1, \ldots, y_n : A_n \vdash u \vdash B \). We claim that \( y_1 : A_1, \ldots, y_n : A_n \vdash \langle t, u \rangle \vdash A \land B \).

Given \( m_1, \ldots, m_k \in \mathbb{N} \) and \( u_1 \vdash A_1[m_1/x], \ldots, u_n \vdash A_n[m_n/x] \), we have \( \langle t, u \rangle[m_1/x, u_1/y] = \langle t[m_1/x], u_1/y \rangle \), and we are done with Lem. 8.35 since \( t[m_1/x, u_1/y] \vdash A[m_1/x] \) and \( u[m_1/x, u_1/y] \vdash B[m_1/x] \).

Case of
\[ (\land \mathbf{E}) \quad \Delta \vdash A_1 \land A_2 \quad \frac{}{\Delta \vdash A_i} \]

By induction hypothesis, we get \( y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A_1 \land A_2 \). We directly get \( y_1 : A_1, \ldots, y_n : A_n \vdash \pi_i t \vdash A_i \).

Case of
\[ (\forall \mathbf{I}) \quad \Delta \vdash A \quad \frac{\Delta \vdash (\forall x)A (x \notin \text{FV}(\Delta))}{\Delta \vdash A[A/x]} \]

By induction hypothesis, we get \( y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A \) with \( x_1 : \text{nat}, \ldots, x_k : \text{nat}, x : \text{nat}, y_1 : A_1, \ldots, y_n : A_n \vdash t : A_1 \). We claim that \( y_1 : A_1, \ldots, y_n : A_n \vdash \lambda x.t \vdash (\forall x)A \).

Recalling that \( x \) is not free in the \( A_i \)'s, let \( m_1, \ldots, m_k \in \mathbb{N} \) and \( u_1 \vdash A_1[m_1/x], \ldots, u_n \vdash A_n[m_n/x] \). We have to show that \( \langle \lambda x.t \rangle[m_1/x, u_1/y] \vdash (\forall x)A[m_1/x] \). But given \( m \in \mathbb{N} \), the induction hypothesis implies \( t[m_1/x, m/x, u_1/y] \vdash A[m_1/x, m/x] \), and we conclude with Lem. 8.35.

Case of
\[ (\forall \mathbf{E}) \quad \Delta \vdash (\forall x)A \quad \frac{}{\Delta \vdash A[A/x]} \]

The induction hypothesis gives \( y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash (\forall x)A \). We can assume w.l.o.g. that \( a \) has free variables among \( x_1, \ldots, x_k \). By Prop. 8.16 (§8.2.3), there is a term \( a \) of System T which represents \( \llbracket a \rrbracket : \mathbb{N}^k \to \mathbb{N} \). We claim that \( y_1 : A_1, \ldots, y_n : A_n \vdash t a \vdash A[a/x] \).

Let \( m_1, \ldots, m_k \in \mathbb{N} \) and \( u_1 \vdash A_1[m_1/x], \ldots, u_n \vdash A_n[m_n/x] \). Further, let \( n := \llbracket a \rrbracket(m) \). The induction hypothesis gives \( \langle t[m_1/x, u_1/y] \rangle \vdash \langle A[m_1/x, n/x] \rangle \). By Lem. 8.34 we get \( \langle t[m_1/x, u_1/y] \rangle \vdash \langle A[m_1/x, a[m_1/x]/x] \rangle \), and we are done with Lem. 8.35 since by definition of \( a \) we have \( \langle t a \rangle[m_1/x, a[m_1/x]/x] \rangle \vdash A[m_1/x, a[m_1/x]/x] \).

Case of
\[ (\exists \mathbf{I}) \quad \Delta \vdash A[a/x] \quad \frac{}{\Delta \vdash (\exists x)A} \]

The induction hypothesis gives \( y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash A[a/x] \). We can assume w.l.o.g. that \( a \) has free variables among \( x_1, \ldots, x_k \). By Prop. 8.16 (§8.2.3), there
8. Gödel’s System $T$

is a term $a$ of System $T$ which represents $\llbracket a \rrbracket : \mathbb{N}^k \rightarrow \mathbb{N}$. We claim that $y_1 : A_1, \ldots, y_n : A_n \vdash \langle a, t \rangle \vdash (\exists x)A$. Let $m_1, \ldots, m_k \in \mathbb{N}$ and $u_1 \vdash A_1[\overline{m}]/\overline{x}], \ldots, u_n \vdash A_n[\overline{m}]/\overline{x}]$. Further, let $n := \llbracket a \rrbracket (\overline{m})$. By induction hypothesis we have $t[\overline{m}]/\overline{x}, \overline{u}/\overline{y}] \vdash A[\overline{m}]/\overline{x}, \overline{a}/\overline{y}]$, from which Lem. 8.34 gives $t[\overline{m}]/\overline{x}, \overline{u}/\overline{y}] \vdash A[\overline{m}]/\overline{x}, \overline{n}/\overline{x}]$. Then we are done with Lem. 8.35 since $\pi_1(a, t)[\overline{m}/\overline{x}, \overline{u}/\overline{y}] \triangleright^{*} n$ while $\pi_2(a, t)[\overline{m}/\overline{x}, \overline{u}/\overline{y}] \triangleright^{*} t[\overline{m}/\overline{x}, \overline{u}/\overline{y}] \vdash A[\overline{m}]/\overline{x}, \overline{n}/\overline{x}]$.

Case of

\[(\exists\text{-E}) \quad \Delta \vdash (\exists x)A \quad \Delta, A \vdash B \quad (x \notin \text{FV}(\Delta, B))\]

The induction hypotheses give $y_1 : A_1, \ldots, y_n : A_n \vdash t \vdash (\exists x)A$ and $y_1 : A_1, \ldots, y_n : A_n, y : A \vdash u \vdash B$, with $x_1 : \text{nat}, \ldots, x_k : \text{nat}, x : \text{nat}, y_1 : A_1^\circ, \ldots, y_n : A_n^\circ \vdash u : B^\circ$. We claim that $y_1 : A_1, \ldots, y_n : A_n \vdash u[t[\pi_1 t/x][\pi_2 t/y]] \vdash B$.

Recalling that $x$ is not free in the $A_i$’s, let $m_1, \ldots, m_k \in \mathbb{N}$ and $u_1 \vdash A_1[\overline{m}]/\overline{x}], \ldots, u_n \vdash A_n[\overline{m}]/\overline{x}]$. We have to show that $u[\pi_1 t/x][\pi_2 t/y][\overline{m}/\overline{x}, \overline{u}/\overline{y}] \vdash B$. But we are done by induction hypothesis on $u$ since the induction hypothesis on $t$ gives $t[\overline{m}/\overline{x}, \overline{u}/\overline{y}] \vdash A[\overline{m}/\overline{x}, \pi_1 t[\overline{m}/\overline{x}, \overline{u}/\overline{y}]/\overline{x}]/\overline{x}$.

We now turn to the Equality Rules of Fig. 15 ($\text{§6.4.2}$), namely:

\[(\doteq\text{-I}) \quad \Delta \vdash a \doteq a \quad (\doteq\text{-E}) \quad \Delta \vdash a \doteq b \quad \Delta \vdash A[a/x] \quad \Delta \vdash a \doteq b \quad \Delta \vdash A[b/x]\]

Via Ex. 6.60 ($\text{§6.4.2}$), we are done with the following.

**Lemma 8.42.** Let $a, b$ be closed first-order terms and let $A$ be a formula with at most $x$ free.

1. $\langle \rangle \vdash a \doteq a$

2. $\lambda x.\lambda x. A \vdash a \doteq b \Rightarrow A[a/x] \Rightarrow A[b/x]$

**Proof.** Exercise! $\square$

It remains to deal with the non-logical rules of HA ($\text{§7.2.4}$). The case of Non-Confusion 7.2.4.(1) was handled in Ex. 8.33, while each Equational Axiom 7.2.4.(3) is realized by a term of the form $\lambda \overline{x}.\langle \rangle$, where $\overline{x}$ has the same length as the corresponding prenex universal quantifier. We handle the Induction Scheme 7.2.4.(2) separately.

**Lemma 8.43.** Let $A$ be a formula with at most $x$ free. Then

$\lambda y.\lambda z.\lambda x. \text{Rec}(y, z, x) \vdash A[0/x] \Rightarrow (\forall y)(A[y/x] \Rightarrow A[Sy/x]) \Rightarrow (\forall x)A$

**Proof.** Let $u \vdash A[0/x]$ and $v \vdash (\forall y)(A[y/x] \Rightarrow A[Sy/x])$. By Lem. 8.35, it is sufficient to show that $\text{Rec}(u, v, 0) \vdash A[0/x]$ for all $n \in \mathbb{N}$. We reason by induction on $n \in \mathbb{N}$.

**Base Case.**

By Lem. 8.35, since $\text{Rec}(u, v, 0) \triangleright^{*} u \vdash A[0/x]$. 

132
8. Gödel’s System T

Induction Step.

Assume $\text{Rec}(u,v,u) \vDash A[n/x]$. Then we are done by using Lem. 8.35 (again), since $\text{Rec}(u,v,u+1) \vDash_\beta v_n \text{Rec}(u,v,u) \vDash A[S_n/x]$.

This concludes the proof of Prop. 8.39 (and thus of Thm. 8.36 as well).

8.3.2. Extension to Primitive Disjunctions

It is actually possible to directly handle the full language of HA, without relying on the coded disjunction

$$A \lor B := (\exists z)[((z \neq 0) \Rightarrow A) \land (\neg (z \neq 0) \Rightarrow B)]$$

(neither at the level of formulae nor at the level of realizability). To this end, one can consider a version of System T with sum types. Its terms are given by

$$t,u ::= x \mid \lambda x.t \mid tu \mid (t,u) \mid \pi_1 t \mid \pi_2 t \mid \langle \rangle \mid \text{in}_1 t \mid \text{in}_2 t \mid \text{case } t \{ \text{in}_1 x_1 \mapsto u_1 \mid \text{in}_2 x_2 \mapsto u_2 \} \mid 0 \mid S t \mid \text{Rec}(u,v,t)$$

The types are

$$T,U ::= \text{nat} \mid U \rightarrow T \mid T \times U \mid T + U \mid \text{unit}$$

The erasure map $(-)^0$ is extended to

$$(A \lor B)^0 := A^0 + B^0$$

and realizability for disjunctions is given by

$$t \vDash A \lor B \iff \text{there are } i \in \{1,2\} \text{ and } u_i \vDash A_i \text{ with } t \vDash_\beta \text{in}_i u_i \text{ and } u_i \vDash A_i$$

The extension of Adequacy (§8.3.1) is given by the following.

Lemma 8.44. Given closed formulae $A_1,A_2,B$, we have

1. $\lambda x . \text{in}_i x \vDash A_i \Rightarrow A_1 \lor A_2$
2. $\lambda d . \lambda f_1 . \lambda f_2 . \text{case } d \{ \text{in}_1 x_1 \mapsto (f_1 x_1) \mid \text{in}_2 x_2 \mapsto (f_2 x_2) \} \vDash A_1 \lor A_2 \Rightarrow (A_1 \Rightarrow B) \Rightarrow (A_2 \Rightarrow B) \Rightarrow B$

Proof. Exercise!

Lemma 8.44 easily gives the extension of Prop. 8.39 (as well as Thm. 8.36) to formulae with primitive disjunctions. Note that the realizers in Lem. 8.44 depend only on $A^0_i, B^0$. 

133
8. Gödel’s System T

8.3.3. The Theory of Realized Formulae

An important consequence of the Adequacy Theorem 8.36 is that the set of closed formulae which are realized by (closed) terms of System $T$ forms an intuitionistic theory in the sense of Def. 6.26 (§6.2.2). This theory is consistent since $\bot$ is not realized (by definition). But we shall see that (as claimed in Prop. 7.58, §7.3.3) it nevertheless validates principles which are classically false!

First note the following.

**Lemma 8.45.**

(1) If $A$ is a closed formula, then either $A$ or $\neg A$ is realized, but not both.

(2) If $A$ is a closed $\Sigma^0_1$-formula (§7.3.2), then $A$ is realizable if and only if $A$ is true.

**Proof.**

(1) If $A$ is not realized, then the term $\lambda x.x$ realizes $\neg A$. If $A$ and $\neg A$ were both realized, then we would get a realizer of $\bot$, a contradiction.

(2) Using (primitive recursive) pairing (Ex. 7.12, §7.2.1) and the representation of quantifier-free formulae of $HA$ given by Cor. 7.53 (§7.3.2), we can assume that $A$ is of the form $(\exists x)(a(x) = 0)$. Then, if $t \models A$ we have $[a([\pi_1 t])] = 0$ by definition, so that $A$ is true. Conversely, if $A$ is true, then there some $n \in \mathbb{N}$ such that $[a(n)] = 0$, and $\langle n, \langle \rangle \rangle \models A$. □

As a consequence of Lem. 8.45, we have that $A \lor \neg A$ is always realized for a closed formula $A$. One may thus think that the intuitionistic theories induced by realizability are in fact classical. But this is not the case, because Lem. 8.45 in general fails for open formulae, so that the universal closure of $A \lor \neg A$ is in general not realized, in the sense that assuming $\text{FV}(A) \subseteq \{x_1, \ldots, x_n\}$, we may have that

$$(\forall x_1, \ldots, x_n)(A \lor \neg A)$$

has no realizer. In this case, by Lem. 8.45, the following formula is realized:

$$\neg(\forall x_1, \ldots, x_n)(A \lor \neg A)$$

**Proposition 8.46** (Prop. 7.58). The following formula is realized by a (closed) term of System $T$:

$$\neg(\forall xy)((\exists zz' T(x, y, z, z') \lor \neg(\exists zz' T(x, y, z, z')))$$

**Proof.** By definition of realizability for negated formulae, it is sufficient to show that the formula

$$(\forall xy)((\exists zz' T(x, y, z, z') \lor \neg(\exists zz' T(x, y, z, z')))$$

is not realized. Assume toward a contradiction that it admits a realizer $t$ in System $T$. Hence, given $n, m \in \mathbb{N}$,
8. Gödel’s System T

- either \( tn \) reduces to \( in_1 u_1 \), and \( u_1 \) in turns give \( k, \ell \in \mathbb{N} \) such that \( T(n, m, k, \ell) \);
- or \( tn \) reduces to \( in_2 u_2 \) where \( u_2 \) realizes \( (\exists zz')T(n, m, z, z') \). But it follows from Lem. 8.45 that \( (\exists zz')T(n, m, z, z') \) that is realized if and only if it is true, so that (by Lem. 8.45 again), the formula \( (\exists zz')T(n, m, z, z') \) is realized if and only if it is true.

As a consequence, the function which takes \( e, m \) to the (weak head) normal form of \( te_f m \) decides the Halting Problem, a contradiction.

**Corollary 8.47.** The following instance of the Double Negation Shift is not realized:

\[
(\forall x) \neg ((\exists zz')T(\pi_1 x, \pi_2 x, z, z')) \Rightarrow \\
\neg (\forall x)((\exists zz')T(\pi_1 x, \pi_2 x, z, z') \lor \neg (\exists zz')T(\pi_1 x, \pi_2 x, z, z'))
\]

**Proof.** Exercise!

**8.3.4. Realizability with Truth**

It follows from Prop. 8.46 (§8.3.3) that not every realizable formula is provable. One can nevertheless obtain the Extraction Theorems for \( \text{HA} \) (Thm. 7.59, §7.3.3 and Thm. 8.18, §8.2.3) using a variant of (modified) realizability called (modified) realizability with truth, and denoted \( t \vdash_t A \). The relation \( t \vdash_t A \) is defined in the same way as \( t \vdash A \) (Fig. 24), but for the following clauses:

\[
t \vdash_t A \Rightarrow B \quad \text{iff} \quad \text{HA} \vdash A \Rightarrow B \quad \text{and for all} \quad u \vdash_t A, \quad \text{we have} \quad tu \vdash_t B
\]

\[
t \vdash_t (\forall x)A \quad \text{iff} \quad \text{HA} \vdash (\forall x)A \quad \text{and for all} \quad n \in \mathbb{N}, \quad tn \vdash_t A[n/x]
\]

(recall that the involved formulae are all closed).

**Lemma 8.48.** If \( t \vdash_t A \) then \( \text{HA} \) proves \( \vdash A \).

**Proof.** Exercise!

The extension of Adequacy (Thm. 8.36 and §8.3.1) is almost direct, but for the cases of the rules (\( \Rightarrow $$I$$) and (\( \forall $$I$$) and of the non-logical rules of \( \text{HA} \) (§7.2.4).

**Proposition 8.49** (Adequacy). From a proof of \( \vdash A \) in \( \text{HA} \) (with \( A \) closed), one can effectively compute a term \( t \) of System T such that \( t \vdash_t A \).

**Proof.** Exercise!

**Corollary 8.50** (Extraction for \( \text{HA} \) (Thm. 7.59, §7.3.3)). In Heyting Arithmetic (HA),

1. from a proof of \( \vdash A_1 \lor A_2 \), with \( A_1, A_2 \) closed, one can effectively compute an \( i \in \{1, 2\} \) and a proof of \( \vdash A_i \);

2. from a proof of \( \vdash (\exists x)A \), with \( (\exists x)A \) closed, one can effectively compute a natural number \( n \in \mathbb{N} \) and a proof of \( \vdash A[n/x] \).
9. Polymorphism

Proof. Exercise!

Corollary 8.51 (Extraction in System T (Thm. 8.18, §8.2.3)). From a proof of \( \vdash (\forall x_1 \ldots x_k)(\exists y)A(x_1, \ldots, x_k, y) \) in HA (where \( A \) has free variables among \( x_1, \ldots, x_k, y \)), one can effectively compute a System T term \( t : \text{nat}^k \rightarrow \text{nat} \) such that for all \( n_1, \ldots, n_k \in \mathbb{N} \), the formula \( A(n_1, \ldots, n_k, [t(n_1, \ldots, n_k)]) \) is provable in HA.

Proof. Exercise!

An internalized version of (modified) realizability with truth is discussed in [Koh08, §5]. Corollary 8.50 can also be proven with a variant “with truth” of Kleene’s Realizability (see e.g. [SU06, Prop. 9.6.6]). A somewhat different proof method is presented in [TvD88a, Chap. 3, §5.6–5.10].

9. Polymorphism

This §9 presents a typed \( \lambda \)-calculus introduced in the 70’s independently by Girard (under the name System F) and by Reynolds (as the Polymorphic \( \lambda \)-Calculus). Girard’s and Reynolds’ motivations were completely different.

The motivation of Reynolds, coming from computer science, was to formalize the notion of Parametric Polymorphism, according to which extending simple types with type variables (ranged over by \( X, Y, Z, \ldots \in \mathcal{V}_T \)) and universal quantifications on type variables (notation \( (\forall X)T \)) makes it possible to uniformly express that a single algorithm can be given several types. Typical examples (building on Ex. 3.1 §3.2.2 and to be developed in §9.1.3 and §9.2.2) are

\[
\text{id} := \lambda x.x : (\forall X)(X \rightarrow X)
\]

as well as the usual polymorphic map function on lists

\[
\text{map} : (\forall X)(\forall Y)((X \rightarrow Y) \rightarrow \text{list}(X) \rightarrow \text{list}(Y))
\]

such that

\[
\text{map } f \ [t_0; \ldots; t_n] = [ft_0; \ldots; ft_n]
\]

We refer to [Pie02, §23] for more on (parametric) polymorphism in (functional) programming languages.

Unlimited extension of simple types with type variables and (universal) type quantification results in a system with a huge expressive power. Besides (polymorphic) lists, one can represent any datatype over a finite signature (see e.g. [GLT89, §11.4]), as well as product and sum types (§4.4). From a logical perspective, the most important case is the polymorphic typing of Church’s numerals (Ex. 3.1, §3.2.2), namely

\[
\mathbb{n} := \lambda z.\lambda s.s^nz : (\forall X)(X \rightarrow (X \rightarrow X) \rightarrow X)
\]

(remark with the simple types of Ex. 4.3, §4.2.1).
9. Polymorphism

Girard introduced System F with a purely logical motivation, namely as a (strongly) normalizing typed λ-calculus for Second-Order Arithmetic (§8.2.3). In particular, Girard has shown that the System F terms of type nat → nat (with nat as above) characterize exactly those partial recursive functions which are provably total in Second-Order Arithmetic (in very much the same way as Gödel’s System T characterizes the provably total functions of First-Order Arithmetic (Thm. 8.20, §8.2.3)). See ?? below, as well as [SU06, §11 & §12] and [GLT89, §11 & §15].

As a consequence of Girard’s characterization, the strong normalization of System F (a result also due to Girard, see [GLT89, §14]) cannot be proven in Second-Order Arithmetic (for very much the same reason as for System T w.r.t. First-Order arithmetic, §8.2.4). This results in a normalization proof which is bound to rely on principles going beyond second-order reasoning, and for which the reducibility machinery of §5 is the only proof method known yet.

System F usually comes under two different presentations, the so-called Church-style and Curry-style ones. In contrast with the simply-typed λ-calculi seen in §4 (but similarly as in the presentation of System T adopted in §8.2.4), in Church-style typed λ-calculi the whole typing derivations are recorded within the λ-terms. In the case of System F, this leads to a system with abstractions and applications for introduction and elimination of universal quantifications on types (in a manner reminiscent from the proof-terms for NJ1 of §6.3). This setting has good type-checking properties, and is a convenient basis for further enrichment with Dependent Types (as in e.g. the Calculus of Constructions, see [SU06, §14] or e.g. [Bar92, §5]).

On the other hand, Curry-style systems record less typing information at the term level (compare the presentation of System T of §8.2 with that of §8.2.4). In the case of System F, this leads to a type system for the pure λ-terms of §3.2.1. Such settings are often better for studying the computational behavior of typed λ-terms, but typically lack decidable type-checking. Besides [SU06, §11.4] (on Curry-style System F), good further readings on Curry-style type systems are [Bar92, §4] and [Kri93].

We refer to [Bar92, §3] for a further discussion of Church-style vs Curry-style typing.

The remaining of this §9 is organized as follows. We present the (original) Church-style System F in §9.1, and the Curry-style version is discussed in §9.2. Finally, strong normalization (for both variants) is proven in §9.3.

Last but not least, logical aspects of System F, namely its strong ties with Second-Order logic, is discussed separately in §??.

9.1. Church-Style System F

Church-style System F (actually the original version of System F) is an explicit version of System F, in the sense that terms contain type annotations. This contrasts with the λ-calculus we have seen so far (which are called Curry-style). These annotations allow Church-style System F to have decidable type-checking (Rem. 9.22, §9.1.4).

Besides [SU06, §11.2], the standard reference is [GLT89, §11].
9. Polymorphism

9.1.1. Definition

Fix a countably infinite set \( V_{TY} = \{X, Y, Z, \ldots\} \) of type variables. The types of System \( F \) are given by the grammar

\[
T, U ::= X \mid U \rightarrow T \mid (\forall X)T
\]

where \( X \in V_{TY} \).

The \( \lambda \)-terms of Church-Style System \( F \) are given by the grammar

\[
t, u ::= x \mid \lambda x : T.t \mid tu \mid \Lambda X.t \mid tT
\]

where \( X \in V_{TY} \) and \( x \in \mathcal{X} \) (§3.2.1).

Note that the syntax of terms depends on types, since besides type abstractions \((\Lambda X.t)\) and type applications \((tT)\), the type of the bound variable is recorded in the usual \( \lambda \)-abstraction \( \lambda x : T.t \).

The notion of free-variable (Def. 3.3, §3.2.3) is adapted so as to encompass the free type variables occurring in a term and in a type.

Definition 9.1 (Free Variable). The sets \( \text{FV}(T) \) and \( \text{FV}(t) \) of free (term or type) variables of \( T \) and \( t \) are defined by induction as follows:

\[
\begin{align*}
\text{FV}(X) & ::= \{X\} \quad & \text{FV}(x) & ::= \{x\} \\
\text{FV}(U \rightarrow T) & ::= \text{FV}(U) \cup \text{FV}(T) \\
\text{FV}(\lambda x : T.t) & ::= \text{FV}(T) \cup \text{FV}(t) \setminus \{x\} \\
\text{FV}((\forall X)T) & ::= \text{FV}(T) \setminus \{X\} \\
\text{FV}(tT) & ::= \text{FV}(t) \cup \text{FV}(T) \\
\text{FV}(\Lambda X.t) & ::= \text{FV}(t) \setminus \{X\}
\end{align*}
\]

Warning 9.2 (Variable Binding). As suggested by Def. 9.1 and similarly as for first-order formulae (§6.1.2), universal quantifiers in types \((\forall X)T\) bind \( X \) in \( T \). We thus assume that System \( F \) types are quotiented by \( \alpha \)-equivalence (w.r.t. the obvious adaptation of §3.2.4). We also assume the obvious adaptation (from §6.1.2) of the notion of capture-avoiding type substitution.

Concerning \( \lambda \)-terms, the variable \( X \) is bound in \( \Lambda X.t \), and we assume the corresponding extension of \( \alpha \)-conversion and of capture-avoiding substitution (§3.2.3 and §3.3.1).

The full (strong) relation \( \triangleright_{\beta} \) of \( \beta \)-reduction is defined in Fig. 25 as the closure of the basic reduction relation \( \triangleright_{0} \) under the indicated congruence rules.

The typing rules of (Church-style) System \( F \) are given in Fig 26, where given \( \mathcal{E} = x_1 : T_1, \ldots, x_n : T_n \), we write \( \text{FV}(\mathcal{E}) \) for \( \text{FV}(T_1) \cup \cdots \cup \text{FV}(T_n) \).

9.1.2. Structural Properties

System \( F \) enjoys the same basic structural properties as the typed \( \lambda \)-calculi seen earlier.

Lemma 9.3 (Structural Properties).
9. Polymorphism

Basic Rules:

\[(\lambda x : T.t)u \stackrel{\beta}{\to} t[u/x]\]
\[(\Lambda X.t)U \stackrel{\beta}{\to} t[U/X]\]

Congruence Rules: \(\triangleright_\beta\) is the closure of \(\triangleright_0\) under the rules

\[
\begin{aligned}
  & t \triangleright_\beta t' & \Leftrightarrow & \quad u \triangleright_\beta u' \\
  & tu \triangleright_\beta t'u' & \Leftrightarrow & \quad \lambda x : T.t \triangleright_\beta \lambda x : T.t'
\end{aligned}
\]

\[
\begin{aligned}
  & t \triangleright_\beta t' & \Leftrightarrow & \quad U \triangleright_\beta U' \\
  & \Lambda X.t \triangleright_\beta \Lambda X.t'
\end{aligned}
\]

Figure 25: Beta-Reduction for Church-Style System \(F\).

\[
\begin{aligned}
  & (\text{VAR}) & \frac{}{E \vdash x : T} ((x : T) \in \mathcal{E}) \\
  & (\to\text{-}1) & \frac{\mathcal{E}, x : U \vdash t : T}{\mathcal{E} \vdash \lambda x : U.t : U \rightarrow T} \\
  & (\to\text{-}E) & \frac{\mathcal{E} \vdash t : U \rightarrow T \quad \mathcal{E} \vdash u : U}{\mathcal{E} \vdash t \rightarrow u : T} \\
  & (\forall\text{-}1) & \frac{\mathcal{E} \vdash t : T \quad (X \notin \text{FV}(\mathcal{E}))}{\mathcal{E} \vdash \Lambda X.t : (\forall X)T} \\
  & (\forall\text{-}E) & \frac{\mathcal{E} \vdash t : (\forall X)T}{\mathcal{E} \vdash t[U/X] : T[U/X]}
\end{aligned}
\]

Figure 26: Typing Rules of Church-Style System \(F\).

(Weakening) If \(E \vdash t : T\) and \(x \notin \text{dom}(\mathcal{E})\) then \(E, x : U \vdash t : T\).

(Contraction) If \(E, x : U, y : U \vdash t : T\) then \(E, x : U \vdash t[x/y] : T\).

(Exchange) If \(E, x : U, E', y : V, E'' \vdash t : T\), then \(E, y : V, E', x : U, E'' \vdash t : T\).

Lemma 9.4 (Substitution).

1. If \(E, x : U \vdash t : T\) and \(E \vdash u : U\) then \(E \vdash t[u/x] : T\).
2. If \(E \vdash t : T\) then \(E[U/X] \vdash t[U/X] : T[U/X]\).

Proposition 9.5 (Subject Reduction). If \(E \vdash t : T\) and \(t \triangleright_\beta u\) then \(E \vdash u : T\).

9.1.3. Examples of Impredicative Codings

We now turn to a series of examples of representation of various types in System \(F\). All these examples strongly rely on (sometimes not prenex) universal type quantification, and for this reason are often called impredicative codings.

Most examples below (but for lists, 9.16–9.18) are impredicative representations of type constructions seen earlier in §4.4 and §8.2. We refer to [SU06, §11.3] for further examples (see also [GLT89, §11.3 – §11.5] and [Pie02, §23]).
9. Polymorphism

Example 9.6 (Polymorphic Identity). Let

\[ \text{id} := \Lambda X. \lambda x : X. x : (\forall X)(X \to X) \]

For each type \( T \) we have

\[ \text{id}\,T \triangleright_{\beta} \lambda x : T. x : T \to T \]

and thus

\[ \text{id}\,T\,t \triangleright_{\beta} (\lambda x : T. x)t \triangleright_{\beta} t \]

Note that

\[ \text{id}\,\text{Id} : \text{Id} \to \text{Id} \]

Example 9.7 (Empty Type). Let

\[ \text{void} := (\forall X)X \]

Note that

\[ E \vdash t : \text{void} \]

We shall see in Prop. 9.24 (§9.1.4) that there is no closed term of type \( \text{void} \).

Example 9.8 (Unit Type). Let

\[ \text{unit} := (\forall X)(X \to X) \]

We have

\[ \langle \rangle := \Lambda X. \lambda x : X. x : \text{unit} \]

Example 9.9 (Booleans). Let

\[ \text{bool} := (\forall X)(X \to X \to X) \]

With

\[ \text{true} := \Lambda X. \lambda x : X. \lambda y : X. x \]
\[ \text{false} := \Lambda X. \lambda x : X. \lambda y : X. y \]

\[ (\text{if } t \text{ then } u \text{ else } v)_{T} := t\,T\,u\,v \]

we have

\[ E \vdash \text{true} : \text{bool} \quad E \vdash \text{false} : \text{bool} \]

\[ E \vdash t : \text{bool} \quad E \vdash u : T \quad E \vdash v : T \]

\[ E \vdash (\text{if } t \text{ then } u \text{ else } v)_{T} : T \]

Moreover, we have

\[ (\text{if } \text{true} \text{ then } u \text{ else } v)_{T} = (\Lambda X. \lambda x : X. \lambda y : X. x)\,T\,u\,v \triangleright_{\beta} u \]
\[ (\text{if } \text{false} \text{ then } u \text{ else } v)_{T} = (\Lambda X. \lambda x : X. \lambda y : X. y)\,T\,u\,v \triangleright_{\beta} v \]
9. Polymorphism

Example 9.10 (Product Types). Given types \( T, U \), let

\[ T \times U := (\forall X)((T \rightarrow U \rightarrow X) \rightarrow X) \]

(where \( X \notin \text{FV}(T, U) \)). Given \( \lambda \)-terms \( t, u \), let

\[
\begin{align*}
\text{pair} \; tu & := \Lambda X. \lambda p : T \rightarrow U \rightarrow X. ptu \\
\pi_1 t & := tT(\lambda x : T, \lambda y : U. x) \\
\pi_2 t & := tU(\lambda x : T, \lambda y : U. y)
\end{align*}
\]

so that

\[
\begin{align*}
\mathcal{E} \vdash t : T & \quad \mathcal{E} \vdash u : U \\
\mathcal{E} \vdash \text{pair} \; tu : T \times U & \quad \mathcal{E} \vdash \pi_1 t : T \\
\mathcal{E} \vdash \pi_2 t : U & \quad \mathcal{E} \vdash t : T \times U \\
\mathcal{E} \vdash u : U & \quad \mathcal{E} \vdash \pi_2 t : U
\end{align*}
\]

Moreover, we have

\[
\pi_1(\text{pair} \; tu) = (\Lambda X. \lambda p : T \rightarrow U \rightarrow X. ptu) T(\lambda x : T, \lambda y : U. x) \uparrow^+ \beta
\]

(\( \pi_2(\text{pair} \; tu) \uparrow^+ \beta\) \( t \))

and similarly

Remark 9.11 (Polymorphic Products). Note that the terms \( \text{pair}, \pi_1, \pi_2 \) of Ex. 9.10 actually depend on the types \( T, U \). Let us make this precise by momentarily writing \( \text{pair}^T, \pi_1^T, \pi_2^T \) for the terms \( \text{pair}, \pi_1, \pi_2 \) of Ex. 9.10.

One can actually define polymorphic versions of pairing and projections, namely (overriding the notations used in Ex. 9.10):

\[
\begin{align*}
\text{pair} & := \Lambda Y. \Lambda Z. \lambda x : Y. \lambda y : Z. \Lambda X. \lambda p : Y \rightarrow Z \rightarrow X. p x y \\
\pi_1 & := \Lambda Y. \Lambda Z. \lambda p : Y \times Z. pY(\lambda x : Y, \lambda y : Z. x) \\
\pi_2 & := \Lambda Y. \Lambda Z. \lambda p : Y \times Z. pZ(\lambda x : Y, \lambda y : Z. y)
\end{align*}
\]

Example 9.12 (Sum Types). Given types \( T, U \), let

\[ T + U := (\forall X)((T \rightarrow X) \rightarrow (U \rightarrow X) \rightarrow X) \]

(where \( X \notin \text{FV}(T, U) \)). Given \( \lambda \)-terms \( t, u \), let

\[
\begin{align*}
\text{inl} \; t & := \Lambda X. \lambda \ell : T \rightarrow X. \ell t \\
\text{inr} \; u & := \Lambda X. \lambda r : U \rightarrow X. r u \\
\text{case} \; V \; t \; u \; v & := tv v
\end{align*}
\]
9. Polymorphism

Note that

\[
\begin{align*}
\mathcal{E} \vdash t : T & \quad \mathcal{E} \vdash u : U \\
\mathcal{E} \vdash \text{inl } t : T + U & \quad \mathcal{E} \vdash \text{inr } u : T + U \\
\mathcal{E} \vdash t : T + U & \quad \mathcal{E} \vdash u : T \rightarrow V \quad \mathcal{E} \vdash v : U \rightarrow V \\
\mathcal{E} \vdash \text{case } V t u v : V
\end{align*}
\]

We have

\[
\text{case } V (\text{inl } t) u v \xrightarrow{+} u t \quad \text{and} \quad \text{case } V (\text{inr } t) u v \xrightarrow{+} v t
\]

Remark 9.13 (Polymorphic Sums). Remark 9.11 extends to sum types, to the effect that we have polymorphic versions of \text{inl}, \text{inr}, \text{case}:

\[
\begin{align*}
\text{inl} & : (\forall XY)(Y \rightarrow X + Y) \\
\text{inr} & : (\forall XY)(Y \rightarrow X + Y) \\
\text{case} & : (\forall XYZ)((X + Y) \rightarrow (X \rightarrow Z) \rightarrow (Y \rightarrow Z) \rightarrow Z)
\end{align*}
\]

Example 9.14 (Natural Numbers). Let

\[
\begin{align*}
nat & := (\forall X)(X \rightarrow (X \rightarrow X) \rightarrow X) \\
n & := \Lambda X. \lambda z : X. \lambda s : X \rightarrow X. s^n z \\
Z & := \Lambda X. \lambda z : X. \lambda s : X \rightarrow X. z \\
St & := \Lambda X. \lambda z : X. \lambda s : X \rightarrow X. s(tXzs) \\
\text{iter } Utuv & := tUuv
\end{align*}
\]

(where \( n \in \mathbb{N} \)). Note that

\[
\begin{align*}
\mathcal{E} \vdash Z : \text{nat} & \quad \mathcal{E} \vdash St : \text{nat} & \quad \mathcal{E} \vdash n : \text{nat} \quad (n \in \mathbb{N}) \\
\mathcal{E} \vdash t : \text{nat} & \quad \mathcal{E} \vdash u : U & \quad \mathcal{E} \vdash v : U \rightarrow U \\
\mathcal{E} \vdash \text{iter } Utuv : U
\end{align*}
\]

We have

\[
\begin{align*}
Sn & \xrightarrow{+} n + 1 \\
\text{iter } Zu u v & \xrightarrow{+} u \\
\text{iter } U(St) u v & = \beta v(\text{iter } Utuv)
\end{align*}
\]

Remark 9.15 (System T Recursor). It is of course possible to represent System T’s Recursor (§8) in Church-style System F, see e.g. [SU06, Prop. 11.3.6] or [GLT89, §11.5.1]. This however cannot be made in “constant time” (w.r.t. the number of \( \beta \)-reduction steps), see Rem. 9.32, §9.2.2 (see also [GLT89, §11.5.1]).

However, the expressive power of System F goes far beyond System T, since the System F terms of type \text{nat} \rightarrow \text{nat} are exactly those partial recursive functions which are provably total in Second-Order Arithmetic. See ?? below, as well as [SU06, §11 & §12] and [GLT89, §11 & §15].
Example 9.16 (Lists). Given a type \( T \), let
\[
\text{list}(T) := (\forall X)(X \to (T \to X \to X) \to X)
\]
(where \( X \notin \text{FV}(T) \)). Given \( \lambda \)-terms \( t_0, \ldots, t_n, t, \ell, u, v \), let
\[
[t_0; \ldots; t_n]_T := \Lambda X. \lambda e : X. \lambda c : T \to X \to X. c t_0 (\ldots (c t_n e))
\]
\[
\text{nil}_T := \Lambda X. \lambda e : X. \lambda c : T \to X \to X. e
\]
\[
\text{cons}_T t \ell := \Lambda X. \lambda e : X. \lambda c : T \to X \to X. c t (\ell X e e)
\]
so that
\[
\begin{array}{llllllll}
\mathcal{E} \vdash t_0 : T & \quad & \mathcal{E} \vdash t_n : T & \quad & \mathcal{E} \vdash \ell : \text{list}(T) & \quad & \mathcal{E} \vdash t : T & \quad & \mathcal{E} \vdash \ell : \text{list}(T) \\
\mathcal{E} \vdash [t_0; \ldots; t_n]_T : \text{list}(T) & \quad & \mathcal{E} \vdash \text{nil}_T : \text{list}(T) & \quad & \mathcal{E} \vdash \text{cons}_T t \ell : \text{list}(T) & \quad & \mathcal{E} \vdash \ell : \text{list}(T) & \quad & \mathcal{E} \vdash u : U & \quad & \mathcal{E} \vdash v : T \to U \to U \\
\mathcal{E} \vdash \text{iter}_T U \ell u v & \quad & \mathcal{E} \vdash \ell : \text{list}(T) & \quad & \mathcal{E} \vdash u : U \\
\end{array}
\]
Moreover,
\[
\begin{align*}
\text{cons}_T t \text{nil}_T & \quad \xrightarrow{+} \quad [t]_T \\
\text{cons}_T t [t_0; \ldots; t_n]_T & \quad \xrightarrow{+} \quad [t; t_0; \ldots; t_n]_T \\
\text{iter}_T U \text{nil}_T u v & \quad \xrightarrow{+} \quad u \\
\text{iter}_T U (\text{cons}_T t \ell) u v & \quad =_{\beta} \quad v t (\text{iter}_T U \ell u v)
\end{align*}
\]

Remark 9.17 (Polymorphic Lists). Similarly as with products (Rem. 9.11) and sums (Rem. 9.13), we also have polymorphic versions of the operations of Ex. 9.16, namely:

\[
\begin{align*}
\text{nil} : & \quad (\forall Y)\text{list}(Y) \\
& \quad := \Lambda Y. \text{nil}_Y \\
\text{cons} : & \quad (\forall Y) (Y \to \text{list}(Y) \to \text{list}(Y)) \\
& \quad := \Lambda Y. \lambda x : Y. \lambda y : \text{list}(Y). \text{cons}_Y x y \\
\text{iter} : & \quad (\forall Y) (\forall Z) ((\text{list}(Y) \to Z \to (Y \to Z \to Z) \to Z) \\
& \quad := \Lambda Y. \Lambda Z. \lambda x : \text{list}(Y). \lambda y : Z. \lambda z : Y \to Z \to Z. \text{iter}_Y Z x y z
\end{align*}
\]

Exercise 9.18. Give a polymorphic
\[
\text{map} : (\forall X) (\forall Y)((X \to Y) \to \text{list}(X) \to \text{list}(Y))
\]
such that
\[
\text{map } T U f [t_0; \ldots; t_n]_T \xrightarrow{+} [f t_0; \ldots; f t_n]_U
\]

Proof. Exercise!

Remark 9.19 (Further Examples). Actually, any type of finite structures (together with its induction principle) specified by a finite first-order signature is representable in System \( F \), see \( [GLT89, \S 11.4] \). See also \( [GLT89, \S 11.5.4] \) for a representation of (finite) trees whose branching type is a fixed arbitrary type \( T \) of System \( F \).
9. Polymorphism

9.1.4. Main Properties

The main property of System F is the strong normalization of typable terms. This non-trivial result, due to Girard, is proven in §9.3 (see [GLT89, §14]).

**Theorem 9.20** (Strong Normalization (Girard)). If $\Gamma \vdash t : T$ then $t$ is strongly normalizing for $\triangleright_\beta$.

As usual with non-pure normalizing typed λ-calculi, we obtain confluence via Newman’s Lemma 3.35 (§3.4.3).

**Theorem 9.21** (Confluence). For each typing context $\Gamma$ and each type $T$, the relation $\triangleright_\beta$ is confluent on $|\Gamma\vdash T|$ (where $|\Gamma\vdash T|$ is defined as in Rem. 4.11, §4.2.2).

Explicit type annotations in terms make type-checking decidable in the following sense.

**Remark 9.22** (Decidability of Typing). The following problem is decidable:

- Given a type $T$, a context $\Gamma$ and a Church-style λ-term $t$, decide whether $\Gamma \vdash t : T$ in Church-style System F.

Note that in contrast with Rem. 4.13 (§4.2.2, on the pure simply-typed λ-calculus), it is undecidable whether a given term is typable (in the sense of §4.2.1), see [SU06, §11.2].

A perhaps surprising but non-trivial fact is that type inhabitation is undecidable for System F (see [SU06, §11.6]).

We now turn to the analysis of typed normal forms. The analogue of Lem. 4.33 (§4.4.4) is the following.

**Lemma 9.23** (Typed Normal Forms). If $t$ is a λ-term in $\beta$-normal form and typable in the empty context, then $t$ is of one of the following forms:

$$\lambda x : T. u \quad \text{or} \quad \Lambda X. u$$

Lemma 9.23 is proven by a syntactic analysis similar to the proof of Lem. 4.33. Note that the term $t$ is not assumed to be closed: the assumption that $t$ is typable in the empty context implies that $t$ contains no free λ-variable $x \in X$, but $t$ may contain free type variables $X \in \mathcal{V}_{Ty}$.

The following Prop. 9.24 consists of (not all direct) consequences of Lem. 9.23. Actually, when it comes to the impredicative codings of §9.1.3, the analysis of typed normal forms in the empty context is more intricate than for the simply-typed versions (Lem. 4.33, §4.4.4). We come back on this in Rem. 9.38 (§9.2.3) below.

**Proposition 9.24.**

1. There is no term $t$ such that $\vdash t : \text{void}$.
2. If $\vdash t : \text{unit}$ is a $\beta$-normal form then $t = \emptyset$.
3. If $\vdash t : \text{bool}$ is a $\beta$-normal form then either $t = \text{true}$ or $t = \text{false}$.
4. If $\vdash t : \text{nat}$ is a $\beta$-normal form then $t = n$ for some $n \in \mathbb{N}$.

**Proof.** Exercise! □

144
9. Polymorphism

\[(VAR) \quad E \vdash x : T \quad ((x : T) \in E)\]

\[(\to-I) \quad \frac{E, x : U \vdash t : T}{E \vdash \lambda x.t : U \to T} \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \}
9. Polymorphism

\[ |x| := x \]
\[ |\lambda x : T.t| := \lambda x.|t| \]
\[ |t u| := |t| |u| \]
\[ |\Lambda X.t| := |t| \]
\[ |T| := |t| \]

Figure 28: Erasure from Church-Style to Curry-Style System \( F \).

**Proposition 9.26** (Typability).

1. If \( \mathcal{E} \vdash t : T \) in Church-style System \( F \), then \( \mathcal{E} \vdash |t| : T \) in Curry-style System \( F \).

2. If \( \mathcal{E} \vdash t : T \) in Curry-style System \( F \), then there is a Church-style \( \lambda \)-term \( u \) such that \( |u| = t \) and \( \mathcal{E} \vdash u : T \) in Church-style System \( F \).

9.2.2. Examples of Polymorphic Typings of Pure Lambda-Terms

It follows from §9.2.1 that the Curry-style System \( F \) has the same expressive power as the Church-style version. In particular, all examples for Church-style System \( F \) (§9.1.3) erase to examples for the Curry-style version. We just note here that in the relevant cases, this yields suitable polymorphic types for the pure \( \lambda \)-terms of Ex. 3.1 (§3.2.2).

**Example 9.27** (Polymorphic Identity). Example 9.6 erases to

\[ \text{id} := \lambda x.x : (\forall X)(X \to X) \]

with

\[ \text{id} t \vdash_{\beta} t \]

**Example 9.28** (Booleans). Example 9.9 erases to

\[ \tilde{\mathcal{E}} \vdash T : \text{bool} \quad \tilde{\mathcal{E}} \vdash F : \text{bool} \]
\[ \mathcal{E} \vdash t : \text{bool} \quad \mathcal{E} \vdash u : T \quad \mathcal{E} \vdash v : T \]
\[ \mathcal{E} \vdash \text{if } t \text{ then } u \text{ else } v : T \]

where

\[ \text{bool} := (\forall X)(X \to X \to X) \]
\[ T := \lambda x.\lambda y.x \]
\[ F := \lambda x.\lambda y.y \]
\[ \text{if } t \text{ then } u \text{ else } v := tuv \]

Moreover, we have

\[ \text{if } T \text{ then } u \text{ else } v = (\lambda x.\lambda y.x)uv \vdash_{\beta}^{+} u \]
\[ \text{if } F \text{ then } u \text{ else } v = (\lambda x.\lambda y.y)uv \vdash_{\beta}^{+} v \]
9. Polymorphism

Example 9.29 (Product Types). Example 9.10 erases to

\[
\begin{align*}
\mathcal{E} \vdash t : T & \quad \mathcal{E} \vdash u : U \\
\mathcal{E} \vdash \text{pair } tu : T \times U & \quad \mathcal{E} \vdash \pi t : T \\
\mathcal{E} \vdash \pi t : T & \quad \mathcal{E} \vdash \pi t : U
\end{align*}
\]

where

\[
T \times U := (\forall X)((T \to U \to X) \to X)
\]

\[
\text{pair } tu := \lambda p. ptu
\]

\[
\pi t := t(\lambda x.\lambda y.x)
\]

\[
\pi t := t(\lambda x.\lambda y.y)
\]

Moreover, we have

\[
\pi_1(\text{pair } tu) = (\lambda p. ptu)(\lambda x.\lambda y.x) \triangleright^\beta t
\]

\[
\pi_2(\text{pair } tu) = (\lambda p. ptu)(\lambda x.\lambda y.y) \triangleright^\beta u
\]

Example 9.30 (Church’s Numerals). Example 9.14 erases to

\[
nat := (\forall X)(X \to (X \to X) \to X)
\]

\[
0 := \lambda z.\lambda s.sz \quad \lambda z.\lambda s.z
\]

\[
S := \lambda x.\lambda z.\lambda s. s(xzs) \quad \text{iter } tuv := t uv
\]

(where \(n \in \mathbb{N}\)). We have

\[
\begin{align*}
\mathcal{E} \vdash 0 : \text{nat} \quad \mathcal{E} \vdash S : \text{nat} \to \text{nat} \quad \mathcal{E} \vdash n : \text{nat} \quad (n \in \mathbb{N})
\end{align*}
\]

and

\[
\begin{align*}
S n & \triangleright^\beta n + 1 \\
\text{iter } 0 uv & \triangleright^\beta u \\
\text{iter } (S t) uv =_\beta v(\text{iter } t uv)
\end{align*}
\]

Exercise 9.31. Give terms

\[
\begin{align*}
\text{add} : \text{nat} \to \text{nat} \to \text{nat} \\
\text{mult} : \text{nat} \to \text{nat} \to \text{nat} \\
\text{exp} : \text{nat} \to \text{nat} \to \text{nat}
\end{align*}
\]

such that

\[
\begin{align*}
\text{add } n m & \triangleright^\beta n + m \\
\text{mult } n m & \triangleright^\beta n \times m \\
\text{exp } n m & \triangleright^\beta n^m
\end{align*}
\]

Proof. Exercise!
9. Polymorphism

Remark 9.32 (System T Recursor). Remark 9.15 (§9.1.3) implies that it is of course possible to represent System T’s Recursor (§8) in Curry-style System F (see e.g. [SU06, Prop. 11.3.6]). This however cannot be made in constant time ([Par89]), in the sense that there is no (pure) \( \lambda \)-term \( \text{Rec} \) such that there is \( k \in \mathbb{N} \) such that for all \( \lambda \)-terms \( t, u, v \in \Lambda \) we have

\[
\text{Rec } u v 0 \overset{k}{\to} u \quad \text{and} \quad \text{Rec } u v (St) \overset{k}{\to} v t (\text{Rec } u v t)
\]

Remark 9.33 (Polymorphic Versions). Similarly as in Rem. 9.11 (§9.1.3) we also have polymorphic versions of Ex. 9.28, Ex. 9.29 and Ex. 9.30. Namely

\[
\begin{align*}
\lambda x.\lambda y. \text{pair } x y &= \lambda x.\lambda y.\lambda p. p x y : (\forall XY)(X \to Y \to X \times Y) \\
\lambda p. \pi_i x &= \lambda p. p (\lambda x_1.\lambda x_2. x_i) : (\forall X_1 X_2)(X_1 \times X_2 \to X_i)
\end{align*}
\]

and

\[
\begin{align*}
\lambda b.\lambda x.\lambda y. \text{if } b \text{ then } x \text{ else } y &= \lambda b.\lambda x.\lambda y. b x y : (\forall X)(\text{bool} \to X \to X \to X) \\
\lambda x.\lambda y.\lambda z. \text{iter } x y z &= \lambda x.\lambda y.\lambda z. x y z : (\forall X)(\text{nat} \to X \to (X \to X) \to X)
\end{align*}
\]

9.2.3. Main Properties

A striking aspect of Curry-style System F is that a given term can be given many types. For instance (with the notations of Ex. 9.27, §9.2.2):

\[
\begin{align*}
id : &\quad \text{Id} \\
id : &\quad \text{Id} \to \text{Id} \\
id : &\quad (\text{Id} \to \text{Id}) \to (\text{Id} \to \text{Id}) \\
id : &\quad \cdots
\end{align*}
\]

This cannot happen in the Church-style version, since typing of Church-style \( \lambda \)-terms is syntax-directed: there is at most one typing derivation for given term (in a given typing environment).

In contrast, typing in Curry-style System F is not syntax-directed. This fact (which may be seen as an actual feature of the Curry-style version, as in e.g. [Kri93, §8–§10]) makes typing somehow more difficult with the Curry-style version than with the Church-style one. A typical instance of this is Subject Reduction, for which we refer to [SU06, §11.4] (see also [Kri93, §8.2] or [Bar92, §4.2]).

Theorem 9.34 (Subject Reduction). In Curry-style System F, if \( E \vdash t : T \) and \( t \overset{\beta}{\to} u \) then \( E \vdash u : T \).

Typed Curry-style terms are strongly normalizing.

Theorem 9.35 (Strong Normalization). In Curry-style System F, if \( E \vdash t : T \) then \( t \) is strongly normalizing for \( \overset{\beta}{\to} \).

We prove Thm. 9.35 in §9.3. We shall actually deduce the Strong Normalization for the Church-style version (Thm. 9.20, §9.1.4) from Thm. 9.35.
9. Polymorphism

Remark 9.36 (Undecidability of Typing). The following problem is **undecidable**:

- Given a type $T$, a context $E$ and a $\lambda$-term $t$, decide whether $E \vdash t : T$ in Curry-style System $F$.

This result, which is not as easy as it may seems, is due to Wells ([SU06, Thm. 11.4.7]).

The analogue of Prop. 9.24 (§9.1.4) for Curry-style terms is the following (with the notations of §9.2.2), which can be proven from Prop. 9.24 via the erasure map of §9.2.1.

**Proposition 9.37.**

1. There is no term $t$ such that $\vdash t : \text{void}$.
2. If $\vdash t : \text{unit}$ is a $\beta$-normal form then $t = \text{id}$.
3. If $\vdash t : \text{bool}$ is a $\beta$-normal form then either $t = \text{T}$ or $t = \text{F}$.
4. If $\vdash t : \text{nat}$ is a $\beta$-normal form then $t = n$ for some $n \in \mathbb{N}$.

Remark 9.38 (Analysis of Closed Typed Normal Forms). Note that neither Prop. 9.37 nor Prop. 9.24 (§9.1.4) deal with the impredicative coding of product types (nor with that of sum types).

As alluded to before Prop. 9.24 (§9.1.4), regarding the impredicative codings of §9.1.3 and §9.2.2, the analysis of closed typed normal forms of System $F$ is more intricate than in the simply typed case.

We refer to [Kri93, §8.4] for a general theory of “data-types” which makes it possible to obtain the expected results in Curry-style System $F$. For instance, under suitable assumptions on $U$ and $V$, the machinery of [Kri93, §8.4] gives the following (with the notation of §9.2.2):

- If $\vdash t : U \times V$ is a $\beta$-normal form then $t = \text{pair } u v$ with $\vdash u : U$ and $\vdash v : V$.

9.3. Strong Normalization

We prove here that the typed terms of Church-style and Curry-style System $F$ are strongly normalizing. We follow the same general outline as [SU06, §11.5]. Other important references are [Kri93, §8.3] (as well as [Bar92, §4.3]), and of course [GLT89, §14].

**Theorem 9.39 (Girard).**

1. If $t$ is typable term of Church-style System $F$, then $t$ is strongly normalizing.
2. If $t$ a pure $\lambda$-term typable in Curry-style System $F$, then $t$ is strongly normalizing.

Theorem 9.39.(1) follows from Thm. 9.39.(2) using a combinatorial argument (actually formalizable in Second-Order Arithmetic) discussed in §9.3.1. The core of Thm. 9.39, namely Thm. 9.39.(2), is proven in §9.3.2 below, using an extension of the reducibility method of §5.
9. Polymorphism

9.3.1. Erasing from Church-style to Curry-style System \( F \)

We show here Thm. 9.39.(1) assuming Thm. 9.39.(2): If Curry-style System \( F \) is strongly normalizing, then so is Church-style System \( F \).

The proof is based on the erasure \(|−|\) of Fig. 27 (§9.2.1). Recall from Prop. 9.26 that \(|−|\) preserves and reflects typability.

Erasing almost preserves reductions. In order to formulate this, we need to split the relation \( \triangleright_\beta \) of \( \beta \)-reduction for Church-style System \( F \) as

\[
\triangleright_\beta = \triangleright_\lambda \cup \triangleright_\Lambda
\]

where \( \triangleright_\lambda \) (resp. \( \triangleright_\Lambda \)) is the closure under the Congruence Rules of Fig. 25 (§9.1.1) of

\[
(\lambda x : T.t)u \triangleright_\lambda t[u/x] \quad \text{resp.} \quad (\Lambda X.t)T \triangleright_\Lambda t[T/X]
\]

**Lemma 9.40** (Reduction and Erasing). Let \( t, u \) be (possibly untyped) terms of Church-style System \( F \). Then,

1. if \( t \triangleright_\lambda u \) then \( |t| \triangleright_\beta |u| \),
2. if \( t \triangleright_\Lambda u \) then \( |t| = |u| \).

**Remark 9.41.** Note that the strong normalization of \( \triangleright_\Lambda \) is trivial (even on non typable terms) since the number of \( \triangleright_\Lambda \)-redexes strictly decreases at each \( \triangleright_\Lambda \)-step.

**Proposition 9.42.** If Curry-style System \( F \) is strongly normalizing then Church-style System \( F \) is also strongly normalizing.

**Proof.** Exercise! \( \Box \)

9.3.2. Strong Normalization of Curry-Style System \( F \)

We prove here Thm. 9.39.(2). We follow the usual (and only known) method of Girard’s reducibility candidates. The general pattern of the method is that of §5 for normalization of the simply-typed \( \lambda \)-calculus, extended in §8.2.2 and §8.2.5 to System \( T \), and similar to the (modified) realizability interpretation of §8.3.

Our argument actually follows the lines of [Kri93, §8.3] (see also [SU06, §11.5] or [Bar92, §4.3]), which is somehow simpler than [GLT89, §14] (as the latter directly proves the strong normalization of Church-style System \( F \)).

**Notation 9.43.** For the remaining of this §9.3, we let \( SN \) stand for strong normalization w.r.t. \( \beta \)-reduction (see Notation 5.24, §5.5.1).

Roughly speaking, the basic idea is the following. Assume that, along the lines of §5, we want to define an interpretation \([T]\) for each type \( T \) of System \( F \). For arrow types \( U \to T \), we can proceed as in §5, and set

\[
[U \to T] := [U] \circ [T]
\]
9. Polymorphism

However, we have a problem in the case of a type quantification $(\forall X)T$. A tentative definition of $\llbracket(\forall X)T\rrbracket$ could be to take the set of all terms $t \in SN$ such that

$$\text{for all type } U, \ t \in \llbracket T[U/X]\rrbracket$$

But this definition is ill-founded since $T[U/X]$ can be $(\forall X)T$ itself! For instance, the above scheme would lead for $\llbracket(\forall X)X\rrbracket$ to take the set of all $t \in SN$ such that

$$\text{for all type } T, \ t \in \llbracket T\rrbracket$$

The solution found by Girard is to define a priori a suitable family of sets $SAT \subseteq P(SN)$, and then to interpret type quantifications $(\forall X)T$ by universal quantifications over $S \in SAT$. For instance, in the case of $(\forall X)T$ this leads to take

$$\llbracket(\forall X)X\rrbracket = \bigcap SAT$$

Technically, a major difference with the setting of §5 is that type interpretations $\llbracket T\rrbracket$ should now be parametrized by type valuations $\rho : V_{TY} \to SAT$.

9.3.3. Reducibility Candidates

We thus arrive to the (then) easy adaptation of §5.5 to Curry-style System F. Consider the following simple notion of elimination context:

$$E[\ ] \in \text{Elim} ::= \ [ ] \mid E[\ ] \ t$$

Similarly as in Notation 5.25 (§5.5.2), write $(t_1, \ldots, t_n) \triangleright_{\beta} (u_1, \ldots, u_n)$ when there is some $i \in \{1, \ldots, n\}$ such that $t_i \triangleright_{\beta} u_i$ and $t_j = u_j$ for all $j \neq i$.

The key Lem. 5.26 and Lem. 5.27 specialize to the following. We refer to §5.5.2 for the proof.

Lemma 9.44. On pure $\lambda$-terms we have the following.

(Weak Standardization) If $E[(\lambda x.t)u] \triangleright_{\beta} v$, then either $v = E[t[u/x]]$ or $v$ is of the form $E'[((\lambda x.t')u')]$ with $(E[\ ], t, u) \triangleright_{\beta} (E'[\ ], t', u')$.

(Weak Head Expansion) If $E[t[u/x]] \in SN$ and $u \in SN$ then $E[(\lambda x.t)u] \in SN$.

The notion of Saturated Set (Def. 5.28, §5.5.3) for pure $\lambda$-terms simplifies to the following.

Definition 9.45 (Saturated Sets). The set $SAT$ of saturated sets is the set of all $A \subseteq SN$ such that

(i) $E[x] \in A$ whenever $E[\ ] \in \text{Elim} \cap SN$, and

(ii) $E[(\lambda x.t)u] \in A$ whenever $u \in SN$ and $E[t[u/x]] \in A$. 

151
Let us first check that $\text{SAT}$ is not empty.

**Lemma 9.46.** $\text{SN} \in \text{SAT}$

**Proof.** Exercise! □

Note also that thanks to the first clause of $\text{SAT}$, saturated sets are not empty, since $S \in \text{SAT}$ implies $x \in S$ for every variable $x \in X$.

We shall interpret System $\text{F}$ types by saturated sets. In order to achieve this, we need the following closure properties of $\text{SAT}$.

**Lemma 9.47.**

1. Given $A, B \in \text{SAT}$, we have $A \rightarrow B \in \text{SAT}$ (where $\rightarrow$ is as in Def. 5.8, §5.3.2).
2. Given $S \subseteq \text{SAT}$, we have $\bigcap S \in \text{SAT}$.

We can finally define the type interpretation. Given $\rho : \mathcal{V}_{\text{Ty}} \rightarrow \text{SAT}$, define $\llbracket T \rrbracket \rho$ by induction on $T$ as follows:

$$
\llbracket X \rrbracket \rho := \rho(X) \\
\llbracket U \rightarrow T \rrbracket \rho := \llbracket U \rrbracket \rho \rightarrow \llbracket T \rrbracket \rho \\
\llbracket (\forall X)T \rrbracket \rho := \bigcap_{S \in \text{SAT}} \llbracket T \rrbracket \rho[S/X]
$$

**Lemma 9.48.** For all type $T$ and all $\rho : \mathcal{V}_{\text{Ty}} \rightarrow \text{SAT}$ we have $\llbracket T \rrbracket \rho \in \text{SAT}$.

**9.3.4. Adequacy**

We now turn to the adequacy of our type interpretation. Recall from Def. 5.7 (§5.3.2) that this amounts to the following:

- If $x_1 : U_1, \ldots, x_n : U_n \vdash t : T$ is derivable in Curry-style System $\text{F}$, then for all $\rho : \mathcal{V}_{\text{Ty}} \rightarrow \text{SAT}$ and all $u_1 \in \llbracket U_1 \rrbracket \rho, \ldots, u_n \in \llbracket U_n \rrbracket \rho$ we have $t[\bar{u}/\bar{x}] \in \llbracket T \rrbracket \rho$.

We need the following “semantic” Substitution Lemma.

**Lemma 9.49 (Substitution).** Given $T, U$ and $\rho : \mathcal{V}_{\text{Ty}} \rightarrow \text{SAT}$, we have $\llbracket T[U/X] \rrbracket \rho = \llbracket T \rrbracket \rho[\llbracket U \rrbracket \rho/X]$.

We now prove the adequacy of the interpretation. We reason by induction on typing derivations and by cases on the last applied rule. In the following, we assume that the contexts $\mathcal{E}$ are of the form $x_1 : U_1, \ldots, x_n : U_n$.

**Case of**

$$
(x : T) \in \mathcal{E} \\
\mathcal{E} \vdash x : T
$$

Trivial.
9. Polymorphism

Case of

\[ (\to.1) \quad \mathcal{E}, x : U \vdash t : T \quad \mathcal{E} \vdash \lambda x.t : U \to T \]

Let \( \bar{u} \in \llbracket U \rrbracket \rho \) and \( u \in \llbracket U \rrbracket \rho \). We have to show \( \lambda x.t[\bar{u}/x]u \in \llbracket T \rrbracket \rho \).

By induction hypothesis we have \( t[\bar{u}/x, u/x] \in \llbracket T \rrbracket \rho \), and we are done since \( \llbracket T \rrbracket \rho \in SAT \) and \( u \in SN \).

Case of

\[ (\to.\text{-}E) \quad \mathcal{E} \vdash t : U \to T \quad \mathcal{E} \vdash u : U \]

\[ \mathcal{E} \vdash tu : T \]

By definition of \( (\to \mathbf{\square}) \to (\to) \).

Case of

\[ (\forall2.1) \quad \mathcal{E} \vdash t : T \quad \mathcal{E} \vdash (\forall X) \quad (X \not\in \text{FV} (\mathcal{E})) \]

Let \( \bar{u} \in \llbracket U \rrbracket \rho \) and \( S \in SAT \). We have to show \( t[\bar{u}/x] \in \llbracket T \rrbracket \rho[S/X] \).

Note that \( X \not\in \text{FV} (\bar{U}) \), so that \( \bar{u} \in \llbracket U \rrbracket \rho[S/X] \), and we are done by induction hypothesis.

Case of

\[ (\forall2.\text{-}E) \quad \mathcal{E} \vdash (\forall X) T \]

\[ \mathcal{E} \vdash t : T[U/X] \]

Let \( \bar{u} \in \llbracket U \rrbracket \rho \). By induction hypothesis we have \( t[\bar{u}/x] \in \llbracket T \rrbracket \rho[\llbracket U \rrbracket \rho/X] \) since \( \llbracket U \rrbracket \rho \in SAT \), and we are done by Lem. 9.49.

We then directly obtain the Strong Normalization Theorem.

**Theorem 9.50** (Thm. 9.39.(2)). If \( \mathcal{E} \vdash t : T \) in Curry-style System \( \textbf{F} \) then \( t \in SN \).

**Proof.** Exercise!
References


References


155
References


References

1988. 7, 10, 11, 12, 16, 17, 18, 37, 54, 63, 75, 76, 77, 78, 79, 94, 95, 96, 97, 101, 105, 107, 109, 110, 111, 127, 136


A. Completeness of Classical Propositional Logic

This Appendix discusses the completeness of the (classical) system NK₀ (Thm. 2.30, §2.3). See §A.4 for a comparison with other usual statements.

A.1. A Semantically Reversible Sequent Calculus

In this §A.1 we show the completeness of a Gentzen-style sequent calculus for a fragment of NK₀. We consider (for simplicity) formulae on the grammar:

\[ A, B ::= p \mid A \Rightarrow B \mid \bot \]

where \( p \) is an atomic proposition. Beware that in contrast with minimal logic (§2.4), we assume the proposition \( \bot \). See [SU06, §7] (also [GLT89, §5], [Bus98a, §1.2] or [Mel09, §1]) for more on Gentzen-style sequent calculi.

Definition A.1.

(1) A **sequent** is a pair \( \Delta \vdash \Gamma \), where \( \Delta \) and \( \Gamma \) are (possibly empty) lists of formulae.

(2) A sequent \( A_1, \ldots, A_n \vdash B_1, \ldots, B_m \) is **valid** if \( (A_1 \land \cdots \land A_n) \Rightarrow (B_1 \lor \cdots \lor B_m) \) is valid (in the sense of Def. 2.10, §2.1.1).

(3) A rule

\[
\begin{array}{c}
\Delta_1 \vdash \Gamma_1 \\
\vdots \\
\Delta_n \vdash \Gamma_n \\
\hline
\Delta \vdash \Gamma
\end{array}
\]

is

- **valid** if the sequent \( \Delta \vdash \Gamma \) is valid whenever the sequents \( \Delta_1 \vdash \Gamma_1, \ldots, \Delta_n \vdash \Gamma_n \) are all valid;
- **semantically reversible** if each sequent \( \Delta_i \vdash \Gamma_i \) is valid whenever the sequent \( \Delta \vdash \Gamma \) is valid.

Remark A.2. Consider a sequent \( A_1, \ldots, A_n \vdash B_1, \ldots, B_m \). If \( n = 0 \), this sequent is valid in the sense of Def. A.1.(2) if and only if the formula \( \top \Rightarrow (B_1 \lor \cdots \lor B_m) \) is valid, that is if and only if \( B_1 \lor \cdots \lor B_m \) is valid. Symmetrically, if \( m = 0 \) the above sequent is valid if and only if \( (A_1 \land \cdots \land A_n) \Rightarrow \bot \) (that is \( \neg (A_1 \land \cdots \land A_n) \)) is valid. As a consequence, the validity of the empty sequent \( \vdash \) (i.e. with \( n = m = 0 \) above) is equivalent to the validity of \( \top \Rightarrow \bot \). It follows that the empty sequent \( \vdash \) is not valid.

We shall consider deduction with the rules of Fig. 29.

Remark A.3. All rules of Fig. 29 are valid.

Lemma A.4. All rules of Fig. 29 are semantically reversible.

Proof. Exercise!
A. Completeness of Classical Propositional Logic

\[
\begin{array}{c}
\Delta, A \vdash A, \Gamma \\
\zeta(\Delta) \vdash \zeta(\Gamma) \\
\Delta, \bot \vdash \Gamma \\
\Delta, \Gamma \Rightarrow B \vdash \Gamma \\
\Delta, A \Rightarrow B, \Gamma \\
\Delta, A \Rightarrow B, \Gamma
\end{array}
\]

Figure 29: A Reversible Sequent Calculus (where \(\zeta\) is a permutation).

**Theorem A.5** (Completeness). If \(\Delta \vdash \Gamma\) is a valid sequent, then \(\Delta \vdash \Gamma\) is derivable with the rules of Fig. 29.

Theorem A.5 can be proved by iteratively applying Lem. A.4 along an induction on the following measure \(|\Delta \vdash \Gamma|\) of sequents \(\Delta \vdash \Gamma\). First, \(|A|\) is defined by induction on \(A\) as

\[
\begin{align*}
|p| & := 0 \\
|\bot| & := 1 \\
|A \Rightarrow B| & := |A| + |B| + 1
\end{align*}
\]

Then let \(|A_1, \ldots, A_n \vdash B_1, \ldots, B_m| := |A_1| + \cdots + |A_n| + |B_1| + \cdots + |B_m|\).

**Proof.** Exercise!

Remark A.6. We stated Thm. A.5 for the logical connectives \(\Rightarrow\) and \(\bot\) only because this is sufficient for the completeness of \(\mathbf{NK}_0\), as the other connectives \((\land, \lor, \top)\) are classically definable from \(\Rightarrow, \bot\) (see Lem. A.10, §A.3 below). But Thm. A.5 actually extends to the full language of \(\mathbf{NK}_0\), using e.g. the following semantically reversible rules:

\[
\begin{array}{c}
\Delta \vdash \Gamma \\
\Delta, \top \vdash \Gamma \\
\Delta \vdash \top, \Gamma \\
\Delta, A, B \vdash \Gamma \\
\Delta, A \land B \vdash \Gamma \\
\Delta \vdash A, \Gamma \\
\Delta \vdash B, \Gamma \\
\Delta \vdash A \lor B, \Gamma \\
\Delta, A \Rightarrow B \vdash \Gamma \\
\Delta, A \lor B \vdash \Gamma
\end{array}
\]

**A.2. Translation to \(\mathbf{NK}_0\)**

We now consider a translation from the classical sequent calculus of Fig. 29 to \(\mathbf{NK}_0\).

**Proposition A.7.** If \(A_1, \ldots, A_n \vdash B_1, \ldots, B_m\) is derivable using the rules of Fig. 29 then \(A_1, \ldots, A_n, \neg B_1, \ldots, \neg B_m \vdash \bot\) is derivable in \(\mathbf{NK}_0\).

**Proof.** Exercise!

Remark A.8. Proposition A.7 extends to the full language of \(\mathbf{NK}_0\) if one extends the sequent calculus of Fig. 29 with the rules of Rem. A.6.
A. Completeness of Classical Propositional Logic

A.3. Completeness of $\text{NK}_0$

We finally show the completeness of $\text{NK}_0$.

**Theorem A.9** (Completeness of $\text{NK}_0$ (Thm. 2.30, §2.3)). *If $\Delta \vdash A$ is a valid sequent (in the language of §2), then it is provable in $\text{NK}_0$.***

We obtain Thm. A.9 from Thm. A.5 and Prop. A.7 via the following, which says that all the formulae of §2 can be defined (w.r.t. classical logic) in the language of §A.1.

**Lemma A.10.** $\text{NK}_0$ proves the following:

1. $\vdash \top \iff (\bot \Rightarrow \bot)$
2. $\vdash (A \land B) \iff ((A \Rightarrow B \Rightarrow \bot) \Rightarrow \bot)$
3. $\vdash (A \lor B) \iff ((A \Rightarrow \bot) \Rightarrow (B \Rightarrow \bot) \Rightarrow \bot)$

**Proof.** Exercise! □

**Proof of Theorem A.9.**

Proof. Exercise! □

A.4. Comparison with other (Compactness and) Completeness Statements

Theorem A.9 is essentially equivalent to [SU06, Thm. 6.1.10] (see also [Bus98a, 1.1.3.(1) & 1.1.4]). A common stronger formulation of completeness for classical propositional logic is e.g. [vD04, Thm. 1.5.13] (see also [Bus98a, 1.1.3.(2)]). In order to state it, we first need to make the following definition, based on [vD04, Def. 1.4.2 & Def. 1.5.2].

**Definition A.11.** Let $\Phi$ be an arbitrary set of formulae.

1. *We write $\Phi \vdash A$ if there are formulae $A_1, \ldots, A_n \in \Phi$ such that $A_1, \ldots, A_n \vdash A$ is derivable in $\text{NK}_0$.***

2. We say that $\Phi$ is inconsistent if $\Phi \vdash \bot$.

3. We say that $\Phi$ is consistent if it is not inconsistent.

Hence a set $\Phi$ of formulae is consistent iff $\Phi \not\vdash \bot$.

**Definition A.12.** Let $\Phi$ be an arbitrary set of formulae.

1. Given a valuation $v$, we write $v \models \Phi$ if $v \models B$ for all $B \in \Phi$.

2. Given a formula $A$, we write $\Phi \models A$ when for every valuation $v$, we have $v \models A$ whenever $v \models \Phi$.

We can now state [vD04, Thm. 1.5.13] (see also [Bus98a, 1.1.3.(2)]).
Theorem A.13. If $\Phi$ is consistent, then there is a valuation $v$ such that $v \models \Phi$.

Note that Thm. A.13 easily gives Thm A.9.

Proof. Exercise!

Theorem A.13 is actually stronger than Thm A.9. This is best seen via the usual (purely model-theoretic) Compactness Theorem for (classical) propositional logic. See e.g. [Bus98a, 1.1.5] (see also [vD04, Ex. 5.8]).

Theorem A.14 (Compactness). If $\Phi \models A$ then there is a finite $\Phi_0 \subseteq \Phi$ such that $\Phi_0 \models A$.

Theorem A.14 should not be confused with the following trivial consequence of Def. A.11.(1):

- If $\Phi \vdash A$, then there is a finite $\Phi_0 \subseteq S$ such that $\Phi_0 \vdash A$.

It is not difficult to see that Thm. A.13 is equivalent to (the conjunction of Thm. A.9 with) Thm. A.14.

Proof. Exercise!

The Compactness Theorem A.14 is the core of Thm. A.13 in terms of infinite combinatorics. It is typically proved using the Prime Ideal Theorem, which itself follows from Zorn’s Lemma, see e.g. [DP02, §10.16–10.19 & §11.16]. The precise statement of [vD04, Thm. 1.5.13] avoids the Prime Ideal Theorem since it restricts to countable languages (but still requires some infinitary combinatorics, see [Sim10, §IV.3]). See also [Bus98a, 1.1.5 & 1.1.6] for further comments.

The name “compactness” for Thm. A.14 suggests connections with topological compactness, and indeed, Thm. A.14 can be seen as a consequence of the compactness of products of compact spaces. The latter result is the famous Tychonoff Theorem, see e.g. [Run05, Thm. 3.3.21] or [Wil70, Thm. 17.8]. See e.g. [Run05, §3.3] or [Wil70, §§8 & §17] for more on topological compactness and product spaces. In its general form, Tychonoff’s Theorem is equivalent to the Axiom of Choice (see e.g. [Wil70, Ex. 17 O] or [Joh82, Notes on §III.1]).

Topological Proof of the Compactness Theorem A.14. It is easy to see that the Compactness Theorem A.14 follows from Tychonoff’s Theorem (see also [Bus98a, 1.1.6]).

Proof. Write AP for the set of atomic propositions. In contrast with Def. 2.10 (§2.1.1) we see valuations $v \subseteq AP$ as characteristic functions $AP \to 2$ (that we still denote $v$).

Consider the product space $2^{AP}$, with 2 discrete (see e.g. [Run05, Def. 3.3.19] or [Wil70, Chap. 3, §8]). It follows from the Tychonoff’s Theorem (see e.g. [Run05, Thm. 3.3.21] or [Wil70, Thm. 17.8]) that $2^{AP}$ is compact since 2 is compact. Note that a given formula $A$ over AP only involves a finite number of propositional variables over AP, so that the set $U_A := \{ v \in 2^{AP} \mid v \models A \}$ is a clopen subset of $2^{AP}$.

161
A. Completeness of Classical Propositional Logic

Assume now that $\Phi \models A$, where $\Phi$ is an arbitrary set of formulae (over AP). Given $v \in 2^{AP}$, note that $v \not\models \Phi$ if and only if $v$ belongs to the open set $\bigcup \{U_B \mid B \in \Phi\}$. Hence, $\Phi \models A$ means that $2^{AP}$ is covered by the family of opens sets $\{U_A\} \cup \{U_B \mid B \in \Phi\}$. Since $2^{AP}$ is compact, it admits a finite subcover, say $\{U_A\} \cup \{U_B \mid B \in \Phi_0\}$ for some finite $\Phi_0 \subseteq \Phi$. But $2^{AP} \subseteq \{U_A\} \cup \{U_B \mid B \in \Phi_0\}$ precisely means that $\Phi_0 \models A$. \qed