CHAPTER 1

Logic

1.1. Computational content of proofs

Mathematics differs from all other sciences by the fact that it provides proofs for its claims. In this course we study what proofs are, and what we can do with them apart from assuring us of the truth of what they state.

Let us start with simple example of a proof. Assume that we already know that $\sqrt{2}$ is irrational.

THEOREM. *There are irrational numbers x, y such that x^y is rational.*

PROOF. By cases.

Case $\sqrt{2}^{\sqrt{2}}$ is rational. Choose $x := \sqrt{2}$ and $y := \sqrt{2}$. Then x, y are irrational and by assumption x^y is rational.

Case $\sqrt{2}^{\sqrt{2}}$ is irrational. Choose $x := \sqrt{2}^{\sqrt{2}}$ and $y := \sqrt{2}$. Then by assumption x, y are irrational and

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

is rational. □

A problem with this proof is that it does not give us an example for what its statement claims to exist. Which pair of real numbers to take depends on whether $\sqrt{2}^{\sqrt{2}}$ is rational or not. As long as we do not know whether this is the case we do not have an example.

An obvious solution to this problem is to extend the standard use of the existential quantifier in mathematics by a new one written $\exists_x A(x)$, whose proof requires an explicit construction of an object x satisfying the property $A(x)$. This in *in addition* to the standard use of the existential quantifier, which we now write as $\tilde{\exists}_x A(x)$ and understand it as $\neg\forall_x \neg A(x)$. The former is called the strong (or constructive) existential quantifier, and the latter the weak (or "classical") one.

Similarly there is a strong (or constructive) disjunction written $A \vee B$, which is in addition to the standard weak (or classical) one. The latter is written $A \tilde{\vee} B$ and understood as $\neg A \to (\neg B \to \bot)$.

Derivation	Term
$u\colon A$	u^A
$\dfrac{\begin{array}{c}[u\colon A]\\ \mid M\\ B\end{array}}{A \to B} \to^+ u$	$(\lambda_{u^A} M^B)^{A\to B}$
$\dfrac{\begin{array}{cc}\mid M & \mid N\\ A \to B & A\end{array}}{B} \to^-$	$(M^{A\to B} N^A)^B$
$\dfrac{\begin{array}{c}\mid M\\ A\end{array}}{\forall_x A} \forall^+ x$ (with var.cond.)	$(\lambda_x M^A)^{\forall_x A}$ (with var.cond.)
$\dfrac{\begin{array}{cc}\mid M & \\ \forall_x A(x) & t\end{array}}{A(t)} \forall^-$	$(M^{\forall_x A(x)} t)^{A(t)}$

TABLE 1. Derivation terms for $\to$ and $\forall$

1.2. Natural deduction

Proofs are done in natural deduction style, following Gentzen (1935). Using the Curry-Howard correspondence we write them as proof terms.

We give an inductive definition of such derivation terms for the $\to, \forall$-rules in Table 1 where for clarity we have written the corresponding derivations to the left. This can be extended to the rules for $\exists$, $\vee$ and $\wedge$, but we will not do this here. The reason is that these connectives will be viewed as inductively defined (nullary) predicates with parameters.

Every derivation term carries a formula as its type. However, we shall usually leave these formulas implicit and write derivation terms without them.

Every derivation term can be written uniquely in one of the forms

$$u\vec{M} \mid \lambda_v M \mid (\lambda_v M)N\vec{L},$$

where u is an assumption variable or constant, v is an assumption or object variable, and M, N, L are derivation or object terms.

1.3. Normal form

An important property of proof terms is that they have a unique normal form. It arises as follows.

A *conversion* removes an elimination immediately following an introduction. We consider the following conversions, for derivations written in tree notation and also as derivation terms.

$\to$-conversion.

$$\dfrac{\dfrac{\begin{array}{c}[u\colon A]\\ \mid M\\ B\end{array}}{A \to B}\to^+ u \qquad \begin{array}{c}\mid N\\ A\end{array}}{B}\to^- \quad \mapsto_\beta \quad \begin{array}{c}\mid N\\ A\\ \mid M\\ B\end{array}$$

or written as derivation terms

$$(\lambda_u M(u^A)^B)^{A\to B} N^A \mapsto_\beta M(N^A)^B.$$

The reader familiar with λ-calculus should note that this is nothing other than β-conversion.

$\forall$-conversion.

$$\dfrac{\dfrac{\begin{array}{c}\mid M\\ A(x)\end{array}}{\forall_x A(x)}\forall^+ x \qquad t}{A(t)}\forall^- \quad \mapsto_\beta \quad \begin{array}{c}\mid M'\\ A(t)\end{array}$$

or written as derivation terms

$$(\lambda_x M(x)^{A(x)})^{\forall_x A(x)} t \mapsto_\beta M(t).$$

The *closure* of the conversion relation $\mapsto_\beta$ is defined by

(a) If $M \mapsto_\beta M'$, then $M \mapsto M'$.
(b) If $M \mapsto M'$, then also $MN \mapsto M'N$, $NM \mapsto NM'$, $\lambda_v M \mapsto \lambda_v M'$ (*inner reductions*).

Therefore $M \mapsto N$ means that M *reduces in one step to* N, i.e., N is obtained from M by replacement of (an occurrence of) a redex M' of M by a conversum M'' of M', i.e., by a single conversion.

A term M is *in normal form*, or M is *normal*, if M does not contain a redex. A *reduction sequence* is a (finite or infinite) sequence $M_0 \mapsto M_1 \mapsto$

$M_2 \ldots$ such that $M_i \mapsto M_{i+1}$, for all i. Finite reduction sequences are partially ordered under the initial part relation; the collection of finite reduction sequences starting from a term M forms a tree, the *reduction tree* of M. The branches of this tree may be identified with the collection of all infinite and all terminating finite reduction sequences. A term is *strongly normalizing* if its reduction tree is finite.

THEOREM 1.3.1. *Every derivation term is strongly normalizing, and the final element of each reduction sequence is uniquely determined.*

A proof can be found for instance in Troelstra and van Dalen (1988).