

## Exercise Sheet 1: Specification and Verification with Higher-Order Logic (Summer Term 2012)

Date: 16.04.2012

### Exercise 1 Calculus of Natural Deduction

We consider the *Genzten-Calculus*, also known as calculus of *natural deduction*. The calculus uses *sequents* (German: *Sequenzen*) of the form  $\Gamma \vdash A$ . They state that the formula  $A$  can be syntactically derived from the set of formulas  $\Gamma$ . If it is possible to derive such a sequent using only the *rules* of the calculus, starting from the *axioms*, we also know that  $A$  is a semantic conclusion from  $\Gamma$  (as the calculus is *correct*).

The calculus has only one axiom, which states that every formula can be derived from itself:  $A \vdash A$ , for all formulas  $A$ . Additionally, there are various rules to derive new sequents from existing ones:

#### Conjunction, Disjunction and Implication (Binary Relations)

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} (\wedge I) \quad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} (\vee I_l) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} (\vee I_r) \quad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} (\rightarrow I)$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} (\wedge E_l) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} (\wedge E_r) \quad \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} (\rightarrow E)$$

$$\frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} (\vee E)$$

#### Truth Values (Constants), Negation (Unary Relation) and Weakening

$$\frac{\Gamma \vdash \text{False}}{\Gamma \vdash A} (\text{False}E) \quad \frac{\Gamma, A \vdash \text{False}}{\Gamma \vdash \neg A} (\neg I) \quad \frac{\Gamma \vdash \neg A \quad \Gamma \vdash A}{\Gamma \vdash \text{False}} (\neg E) \quad \frac{\Gamma \vdash B}{\Gamma, A \vdash B} (W)$$

#### Universal and Existential Quantifiers

$$\frac{\Gamma \vdash \{a_{new}/x\}A}{\Gamma \vdash \forall x.A} (\forall I) \quad \frac{\Gamma \vdash \forall x.A}{\Gamma \vdash \{t/x\}A} (\forall E)$$

$$\frac{\Gamma \vdash \{t/x\}A}{\Gamma \vdash \exists x.A} (\exists I) \quad \frac{\Gamma \vdash \exists x.A \quad \Gamma, \{a_{new}/x\}A \vdash C}{\Gamma \vdash C} (\exists E)$$

The names of the rules are given on the right side in parenthesis. The *I* is an abbreviation of *Introduction*, *E* of *Elimination* and *W* of *Weakening*. The syntax  $\{y/x\}A$  denotes that all unbound occurrences of  $x$  in  $A$  are replaced by  $y$ . You have to choose a completely new variable for each  $a_{new}$ , i.e. it must not appear in any term or formula yet.  $t$  on the other hand is allowed to be an arbitrary term.

A proof in the calculus is a tree of rule applications, whose leaves are axioms and whose root is the theorem you want to prove. Usually such a proof is done *backwards*, starting with the theorem and trying to reach the axioms.

a) (Prepare!) Prove the following sequent using the Gentzen-Calculus:

$$\vdash (a \vee (b \wedge c)) \rightarrow ((a \vee b) \wedge (a \vee c))$$

b) (Prepare!) Prove the following sequent using the Gentzen-Calculus:

$$\vdash \exists x. \forall y. P(x, y) \rightarrow \forall y. \exists x. P(x, y)$$

c) Write an Isabelle/HOL theory for your proofs from a) and b). A skeleton file to start with looks like this:

```
theory Sheet1 imports Main
begin

lemma Exercise_1_a:
"(a \ / (b /\ c)) --> ((a \ / b) /\ (a \ / c))"
apply (rule ...)
...
done

lemma Exercise_1_b:
"(EX x. ALL y. P x y) --> (ALL y. EX x. P x y)"
...

end
```

The rules of the Gentzen-Calculus correspond to the following Isabelle/HOL rules:

Gentzen	Isabelle/HOL	Gentzen	Isabelle/HOL	Gentzen	Isabelle/HOL
$\wedge I$	conjI	$\vee I_l$	disjI1	$\neg I$	notI
$\wedge E_l$	conjunct1	$\vee I_r$	disjI2	$\neg E$	notE
$\wedge E_r$	conjunct2	$\vee E$	disjE	FalseE	FalseE
$\rightarrow I$	impI	$\forall E$	spec	$\exists I$	exI
$\rightarrow E$	mp	$\forall I$	allI	$\exists E$	exE

## Exercise 2 Hilbert-Calculus

The Hilbert-Calculus for propositional logic has only one rule called *modus ponens*:

$$\frac{P \rightarrow Q \quad P}{Q} \text{ (MP)}$$

Additionally, there are three axioms:

(A1)  $P \rightarrow (Q \rightarrow P)$

(A2)  $(P \rightarrow (Q \rightarrow R)) \rightarrow ((P \rightarrow Q) \rightarrow (P \rightarrow R))$

(A3)  $(\neg P \rightarrow \neg Q) \rightarrow (Q \rightarrow P)$

A proof in the Hilbert-Calculus is a sequence of formulas, where each formula is either an axiom, an assumption or the result of using modus ponens on two formulas appearing earlier in the sequence. The sequent  $\Gamma \vdash P$  states that there is a proof using only the assumptions from  $\Gamma$ , which ends in  $P$ .

a) (Prepare!) Proof the sequent  $\vdash b \rightarrow (a \rightarrow a)$  using the Hilbert-Calculus.

b) (Prepare!) Proof the sequent  $\vdash a \vee \neg a$  using the Hilbert-Calculus.

(Hint: You have to eliminate the  $\vee$  first, by expressing it with  $\neg$  and  $\rightarrow$  only.)

c) (Prepare!) Proof the sequent  $\neg\neg a \vdash a$  using the Hilbert-Calculus.

d) Write an Isabelle/HOL theory for these proofs.