Mathematisches Institut
Heinrich-Heine Universität Düsseldorf
Dr. Alexander Bentkamp, Jon Eugster

WiSe 2023/24
5. Dezember 2023

Computer-gestützte Beweisführung

Übungsblatt 7

In allen Aufgaben meinen wir mit „beweisen" die Erstellung formaler Beweisterme. Verwenden Sie keine Taktiken, die nicht in der Vorlesung oder im Skript eingeführt wurden. Zur besseren Klausurvorbereitung empfehlen wir, diese Übungen ohne Lean zu bearbeiten.

Aufgabe 1. Geben Sie eine Typderivation mit den Regeln aus Abschnitt 3.7 des Skripts für die folgenden Terme an:

(a) $\Pi X : \mathsf{Type}.\ \mathsf{False}$
(b) $\Pi X : \mathsf{Type}.\ X$
(c) $\Pi h : \mathsf{False}.\ \mathsf{Prop}$
(d) $\Pi h : \mathsf{False}.\ \mathsf{True}$

Aufgabe 2. Beweisen Sie das Gesetz von Peirce (gesprochen wie englisch „purse")

$$\textbf{theorem}\ \ \mathsf{peirces\_law}\ (p\ q : \mathsf{Prop}) : ((p \to q) \to p) \to p := \ldots$$

mithilfe des Axioms des ausgeschlossenen Dritten

$$\textbf{axiom}\ \ \mathsf{em} : \forall p : \mathsf{Prop}.\ p \lor \neg p$$

Tipp: Machen Sie eine Fallunterscheidung auf $\mathsf{em}\ p$ mittels **match** $\mathsf{em}\ p$ **with**.

Aufgabe 3. Russel's Barbier-Paradoxon lautet:

> Du kannst einen Barbier definieren als „jemanden, der all jene, und nur jene, rasiert, die sich nicht selbst rasieren". Die Frage ist: Rasiert der Barbier sich selbst?

Beweisen Sie, dass ein solcher Barbier zu einem Widerspruch führt. Sei hierzu $\mathsf{Person} : \mathsf{Type}$ der Typ aller Personen und $\mathsf{barbier} : \mathsf{Person}$. Sei $\mathsf{rasiert} : \mathsf{Person} \to \mathsf{Person} \to \mathsf{Prop}$ eine Konstante, wobei „$\mathsf{rasiert}\ x\ y$“ bedeuten soll, dass Person x Person y rasiert.

theorem $\mathsf{barbier\_paradoxon}\ (h : \forall(x : \mathsf{Person}).\ \mathsf{rasiert\ barbier}\ x \leftrightarrow \neg\ \mathsf{rasiert}\ x\ x) :$
$\mathsf{False} := ...$

Tipp: Nutzen Sie das Axiom em. Wenden Sie es auf die Aussage $\mathsf{rasiert\ barbier\ barbier}$ an.

Aufgabe 4. Auf Übungsblatt 5 haben wir das induktive Prädikat Even definiert:

inductive $\mathsf{Even} : \mathsf{Nat} \to \mathsf{Prop} :=$
$\mid \mathsf{base} : \mathsf{Even}\ 0$
$\mid \mathsf{step} : \forall(n : \mathsf{Nat}).\ \mathsf{Even}\ n \to \mathsf{Even}\ (\mathsf{succ}\ (\mathsf{succ}\ n))$

(a) Definieren Sie analog ein Prädikat Odd, das die ungeraden Zahlen $1, 3, 5, ...$ identifiziert. Verwenden Sie dazu nicht das Prädikat Even.

inductive $\mathsf{Odd} : \mathsf{Nat} \to \mathsf{Prop} :=$
$\mid \mathsf{base} : ???$
$\mid \mathsf{step} : ???$

(b) Beweisen Sie, dass $\mathsf{Odd}\ 5$ gilt.

(c) Beweisen Sie das folgende Theorem. Schreiben Sie dabei stets $\mathsf{Even.base}$ / $\mathsf{Odd.base}$ / $\mathsf{Even.step}$ / $\mathsf{Odd.step}$ anstelle von base / step, um Verwechslungen zu vermeiden. Tipp: Induktion.

theorem $\mathsf{odd\_succ\_of\_even}\ (n : \mathsf{Nat}) : \mathsf{Even}\ n \to \mathsf{Odd}\ (\mathsf{succ}\ n)$
$\mid \mathsf{Even.base} \Rightarrow$
show $\mathsf{Odd}\ (\mathsf{succ}\ 0)$ **from** $???$
$\mid \mathsf{Even.step}\ (m : \mathsf{Nat})\ (hm : \mathsf{Even}\ m) \Rightarrow$
show $\mathsf{Odd}\ (\mathsf{succ}\ (\mathsf{succ}\ (\mathsf{succ}\ m)))$ **from** $???$

(d) Beweisen Sie das folgende Theorem.

theorem $\mathsf{even\_succ\_of\_odd}\ (n : \mathsf{Nat}) : \mathsf{Odd}\ n \to \mathsf{Even}\ (\mathsf{succ}\ n)$
???

Abgabe: 12. Dezember 2023, bis 16.30 Uhr auf Ilias
(Oder bei technischen Problemen per Email an `jon.eugster@hhu.de`)
Abgabe zu zweit ist erlaubt.