



Universität Karlsruhe (TH)

Lehrstuhl für Programmierparadigmen

Theorembeweiser und ihre Anwendungen SS 2009 <http://pp.info.uni-karlsruhe.de/>
Übungsleiter: Daniel Wasserrab wasserra@ipd.info.uni-karlsruhe.de

Übungsblatt 10

Besprechung: 30.06.2009

1 Fingerübungen: Quantoren in Isar

Beweisen Sie folgende Aussagen mittels eines strukturierten Beweises in Isar. Sie dürfen zwar automatische Taktiken verwenden, jedoch bitte nicht um das gesamte Lemma zu beweisen, die Beweisidee soll strukturiert aufgeschrieben werden.

Hinweis: wenn Sie eine Aussage und die entsprechend negierte Aussage in Ihren Annahmen haben, können Sie den entsprechenden Ausdruck gleich zu False auswerten lassen mittels der Taktik *contradiction*.

lemma `assumes "∃ x. ∀ y. P x y" shows "∀ y. ∃ x. P x y"`
`oops`

lemma `"(∀ x. P x) = (¬ (∃ x. ¬ P x))"`
`oops`

lemma `"(∀ x. P x → Q) = ((∃ x. P x) → Q)"`
`oops`

lemma `"∃ x. P x → (∀ x. P x)"`
`oops`

2 Rätsel: Der reiche Großvater

Zeigen Sie, dass folgende Aussage gilt:

*Wenn jeder arme Mann einen reichen Vater hat,
dann gibt es einen reichen Mann mit einem reichen Großvater*

theorem `"∀ x. ¬ rich x → rich (father x)
⇒ ∃ y. rich y ∧ rich (father (father y))"`
`oops`

Hinweise:

- Gibt es überhaupt einen reichen Mann?
- Überlegen Sie sich den Beweis erst auf Papier und versuchen Sie ihn dann möglichst analog in Isar zu formulieren
- Sie werden in jedem Fall Fallunterscheidungen brauchen

3 Cantors Theorem

Sie sollen nun Cantors Theorem beweisen; dieses sagt aus, dass es keine surjektive Funktion von einer Menge auf ihre Potenzmenge geben kann. Formalisiert:

theorem " $\exists S. S \notin \text{range } (f :: 'a \Rightarrow 'a \text{ set})$ "

Dabei bezeichnet $\text{range } f$ die Wertemenge einer Funktion.

Hinweise:

- Der Knackpunkt des Beweises ist das Finden der richtigen Menge S . Versuchen Sie es erstmal alleine, erinnern Sie sich (falls bekannt) an das sogenannte *Cantor'sche Diagonalverfahren*. Ansonsten versuchen Sie ihr Glück im Internet, der Name der Übung sollte Hinweis genug sein ;)
- Auch hier sollten Sie sich Ihren Beweis erst auf Papier überlegen und dann möglichst analog in Isar übertragen
- Falls Sie eine Aussage wie $b \in \text{range } f$ haben, lässt sich daraus unmittelbar ein x auswählen ("obtainen"), so dass $b = f x$ gilt, da die Regel rangeE : $\llbracket b \in \text{range } f; \bigwedge x. b = f x \implies P \rrbracket \implies P$ als Eliminationsregel in allen Taktiken des automatischen Schließens existiert