

## Aufgabe 6-1

Im ungetypten  $\lambda$ -Kalkül sei definiert:

$$\begin{aligned} T &::= \lambda x. \lambda y. x \\ F &::= \lambda x. \lambda y. y \\ ite &::= \lambda b. \lambda x. \lambda y. b(x)(y) \\ pair &::= \lambda x. \lambda y. \lambda z. z(x)(y) \\ fst &::= \lambda x. x(T) \\ snd &::= \lambda x. x(F) \\ 0 &::= \lambda x. x \\ s &::= \lambda n. pair(F)(n) \\ iszero &::= fst \\ pred &::= snd \\ Fac &::= \lambda f. \lambda n. ite(iszero(n))(s(0))(mult(n)(f(pred(n)))) \\ Y &::= \lambda f. (\lambda x. f(x(x)))(\lambda x. f(x(x))) \\ fac &::= Y(Fac) \end{aligned}$$

Ferner sei  $mult$  ein Term, so dass für  $m$  und  $n$  von der Form  $0$  oder  $succ(\dots(succ(0))\dots)$  gilt:  $mult(m)(n) = \underbrace{succ(succ(\dots(succ(0))\dots))}_{m*n}$ .

Zeigen Sie:

- a) für alle Terme  $f$  gilt:  $Y(f) = f(Y(f))$
- b)  $fac(0) = s(0)$ ,  $fac(s(x)) = mult(s(x))(fac(x))$
- c)  $fac(s(s(s(0)))) = s(s(s(s(s(0))))))$
- d)  $Y$  lässt sich im einfach getypten  $\lambda$ -Kalkül nicht typisieren.

## Aufgabe 6-2

Seien  $\sigma, \tau, \rho$  Basistypen. Leiten Sie im einfach getypten  $\lambda$ -Kalkül den Typ von

$$\lambda x : (\sigma \rightarrow \tau \rightarrow \rho). \lambda y : (\sigma \rightarrow \tau). \lambda z : \sigma. x(z)(y(z))$$

her.

## Aufgabe 6-3

Gegeben sei folgende Modellierung einer Gruppe in PVS:

```
gruppe : THEORY
BEGIN
  G : TYPE+
  e : G
  i : [G -> G];
  * : [G,G -> G]

  x,y,z : VAR G

  assoziativ : AXIOM (x * y) * z = x * (y * z)
  linksneutral : AXIOM e * x = x
  linksinvers : AXIOM i(x) * x = e
END gruppe
```

Auf der Webseite zur Vorlesung findet sich die Datei `gruppe.pvs`, in der verschiedene Gleichungen aufgelistet sind. (Diese Gleichungen entstehen bei der *Knuth-Bendix-Vervollständigung* des durch die obigen Axiome definierten Termersetzungssystems).

Beweisen Sie mit Hilfe von PVS, dass diese Gleichungen in der Tat aus den Axiomen bzw. den anderen Regeln folgen. Benutzen Sie dazu (ausschließlich!) die Beweiserregeln (SKOLEM!), (REWRITE), und (CASE-REPLACE).

**Hinweis:** Die Beweise verlangen teilweise recht komplexe Termmanipulationen. In der oben erwähnten Datei `gruppe.pvs` sind die Beweise jeweils in mathematischer Notation angegeben. Versuchen Sie, diese in PVS nachzubilden.

## Aufgabe 6-4

In dieser Aufgabe sollen Mengen in PVS durch ihre charakteristischen Prädikate formalisiert werden. Der folgende Ausschnitt aus der Theorie `Sets` formalisiert die Mengenzugehörigkeit und die Gleichheit auf Mengen:

```
Sets : THEORY
BEGIN
  X : TYPE+
  SET : TYPE = [X -> bool] % äquivalent zu: pred[X], set[X] oder setof[X]

  member(x:X,S:SET) : bool = S(x);
  ==(S:SET,T:SET) : bool = FORALL x: member(x,S) IFF member(x,T)
END Sets
```

Die Menge  $S$  wird als ein Prädikat über dem Grundbereich  $X$  (dem Typ der Elemente von  $S$ ) beschrieben. Für ein gegebenes  $x \in X$  ist  $S(x)$  wahr genau dann, wenn  $x$  in der

Menge  $S$  enthalten ist.

Zwei Mengen  $S$  und  $T$  sind gleich, wenn sie die gleichen Elemente besitzen, d. h., wenn ein beliebiges  $x$  zu  $S$  genau dann gehört wenn es auch zu  $T$  gehört.

Als Grundgerüst für diese Aufgabe ist die Datei `Sets.pvs` auf der Webseite zur Vorlesung hinterlegt. In dieser Datei sind auch noch einige Hinweise zu den Teilaufgaben enthalten, die möglicherweise hilfreich sind.

**Hinweis:** Sie kommen in den Beweisen mit den Beweisregeln (SKOSIMP\*), (EXPAND) und (INST?) bzw. deren Varianten und Verwandten, sowie (PROP) und (ASSERT) aus, die in der *Kurzanleitung zu PVS* beschrieben sind.

- a) Definieren Sie die leere Menge `emptyset` und die Menge `fullset`, die alle Elemente enthält, in PVS. Zeigen Sie:

```
empty_no_members : LEMMA NOT member(x, emptyset)
fullset_member   : LEMMA member(x, fullset)
```

- b) Definieren Sie die Mengen `add(x,S)` und `remove(x,S)`, die aus einer Menge  $S$  dadurch entstehen, dass ein Element  $x$  der Menge hinzugefügt bzw. aus ihr entfernt wird. Zeigen Sie:

```
member_add       : LEMMA member(x, add(x, S))
add_idempotent   : LEMMA add(x, add(x,S)) == add(x,S)
member_remove    : LEMMA NOT member(x,remove(x,S))
```

- c) Definieren Sie ein Prädikat `subset?` für die Teilmengenbeziehung zwischen Mengen. Zeigen Sie:

```
subset_emptyset : LEMMA subset?(emptyset, S)
subset_fullset  : LEMMA subset?(S, fullset)
subset_antisymmetric : LEMMA subset?(S, T) AND subset?(T, S) IMPLIES S == T
```

- d) Definieren Sie Operatoren für Schnitt und Vereinigung von Mengen. Zeigen Sie:

```
union_commutative : LEMMA union(S, T) == union(T, S)
union_subset      : LEMMA subset?(S, T) IMPLIES union(S, T) == T
distribute_union_intersection : LEMMA
  union(S, intersection(T, R)) == intersection(union(S, T), union(S, R))
```

- e) Definieren Sie Operatoren für das Komplement einer Menge und die Differenz zweier Mengen. Zeigen Sie:

```
complement_emptyset      : LEMMA complement(emptyset) == fullset
demorgan : LEMMA
  complement(intersection(S,T)) == union(complement(S),complement(T))
difference_fullset       : LEMMA difference(S, fullset) == emptyset
difference_intersection  : LEMMA difference(S,T) == intersection(S,complement(T))
```

- f)** (Optional) Beweisen Sie die auch die zahlreichen Lemmata, die am Ende der Theorie Sets aufgeführt sind. Können Sie in den Beweisen ein gewisses Muster erkennen? Wie könnte eine komplexe Beweisprozedur aussehen, die diese Art von Formeln automatisch beweisen kann?

In der Dokumentation des PVS Beweisersystems sind im Abschnitt 4.12 ab Seite 78 die mächtigeren Beweisstrategien von PVS beschrieben. Lesen Sie deren Dokumentation und versuchen Sie, mit Hilfe der Ihnen geeignet erscheinenden Strategien manche der Lemmata „schneller“ zu beweisen!

## Aufgabe 6-5

In der Vorlesung ist die Definition der Gleichheit wie folgt in der Prädikatenlogik zweiter Stufe angegeben worden:

$$x = y \quad :\Leftrightarrow \quad \forall P : P(x) \Rightarrow P(y)$$

- a)** Definieren Sie diesen Gleichheitsbegriff in PVS. Verwenden Sie für Ihre Gleichheit in PVS das Symbol ==.
- b)** Weisen Sie mit PVS folgende Eigenschaften dieser Gleichheit nach:

- Reflexivität:

$$\forall x : x == x$$

- Transitivität:

$$\forall x, y, z : x == y \wedge y == z \Rightarrow x == z$$

- c)** Weisen Sie die Symmetrie dieser Gleichheit nach:

$$\forall x, y : x == y \Rightarrow y == x$$

Orientieren Sie sich dabei an dem in der Vorlesung vorgestellten Beweis.

- d)** Weisen Sie die Substitutivität dieser Gleichheit nach. Unter Substitutivität versteht man, dass Terme an beliebiger Stelle durch gleiche ersetzt werden können. Wir beschränken uns hier auf das Ersetzen innerhalb von Prädikaten:

$$\forall x, y : x == y \Rightarrow (P(x) \Leftrightarrow P(y))$$