Aufgabe 7-1

Auf der Webseite zur Vorlesung findet sich die Datei `trig.pvs`, die eine einfache Modellierung der trigonometrischen Funktionen *sin* und *cos* enthält.

Beweisen Sie die dort aufgeführten Lemmata. Für die Beweise werden Sie die Regeln `(SKOSIMP*)`, `(EXPAND)` und `(INST?)`, `(CASE)` und `(REPLACE)` (bzw. `(CASE-REPLACE)`) sowie `(LEMMA)`, `(REWRITE)`, `(PROP)` und `(ASSERT)` benötigen. Nehmen Sie die Beschreibung dieser Regeln in der *PVS Kurzanleitung* zu Hilfe.

Gehen Sie wie folgt vor:

a) Beweisen Sie zunächst die Lemmata `sin_2a` und `cos_2a` mit Hilfe der Axiome `sin_plus` bzw. `cos_plus`. Hinweis: $2a = a + a$.

b) Beweisen Sie `sin_0` mit Hilfe von `sin_minus`. Hinweis: $0 = 1 - 1$.

c) Beweisen Sie `sq_sin_cos_one`. Sie benötigen hier die Aussagen `cos_minus` und `cos_0`. Hinweis: $cos(a - a) = cos(0) = 1$.

d) Beweisen Sie `cos_PI2` mittels `sq_sin_cos_one`, `sin_PI2` und `zero_times3`. (Letztere Formel ist Teil der PVS-*Prelude*-Theorie.)

e) Beweisen Sie `cos_PI` und `sin_PI`. Hinweis: $PI = PI/2 + PI/2$.

f) Beweisen Sie `sin_shift` und `cos_shift` mit Hilfe der Lemmata und Axiome der Theorie `trig`.

g) (Optional – Schwierig) Beweisen Sie `exist_cos_ne_0` und `cos_0`.

Aufgabe 7-2

In dieser Aufgabe soll in PVS das Konzept der transitiven Hülle einer binären Relation mit Hilfe von Funktionen und Prädikaten *höherer Stufe* definiert werden.

Den Typ einer binären Relation über einem Basistyp `T` definieren wir in PVS als:

```
T      : TYPE+
BinRel : TYPE = [T,T -> bool]
```

a) Definieren Sie in PVS ein Prädikat `transitive? : [BinRel -> bool]`, so dass `transitive?(R)` genau dann gilt, wenn `R` transitiv ist.

b) Definieren Sie ein Prädikat `<= : [BinRel,BinRel -> bool]`, so dass `R <= S` genau dann gilt, wenn `S` die Relation `R` umfasst.

c) Definieren Sie einen Operator `intersect : [[BinRel -> bool] -> BinRel]`, so dass `intersect(P)` den Schnitt aller Relationen `R` liefert, die das Prädikat `P` erfüllen.

d) Definieren Sie einen Operator `transclosure : [BinRel -> BinRel]`, so dass `transclosure(R)` die transitive Hülle der Relation `R` liefert.

Hinweis: Ein Paar (x, y) ist in der transitiven Hülle einer Relation `R` enthalten, wenn es in *allen* die Relationen , die *transitiv* sind und `R` *umfassen*, enthalten ist.

e) Zeigen Sie, dass ihre Formalisierung der transitiven Hülle tatsächlich die gewünschten Eigenschaften besitzt, nämlich (i) transitiv ist, (ii) `R` umfasst und (iii) die kleinste solche Relation ist.

Hinweis: Für die Eigenschaft (iii) kann es hilfreich sein, ein Prädikat `least? : [pred[BinRel] -> pred[BinRel]]` zu definieren, so dass `least?(P)(R)` genau dann erfüllt ist, wenn `R` die kleinste Relation ist, die `P` erfüllt.

Aufgabe 7-3

a) Definieren Sie die in der Vorlesung vorgestellte Funktion `fakt(n:nat): RECURSIVE nat`, mit $\texttt{fakt}(n) = n!$. Geben Sie dabei eine geeignete Maßfunktion an.

b) Beweisen Sie die auftretenden Typkorrektheitsbedingungen! Die TCCs werden mit dem Kommando `C-c C-q s` oder `M-x show-tccs` angezeigt; der Beweisvorgang wird wie bei anderen Formeln auch durch `M-x pr` gestartet.

c) Formulieren und beweisen Sie ein Theorem für folgende Eigenschaft:

$$\forall\, x > 3 : \texttt{fakt}(x) > 2^x$$

Hinweise:

- Für die Zweierpotenzen 2^x können Sie die in PVS vordefinierte Funktion $\texttt{exp2}(x)$ verwenden.
- Im Beweis benötigen Sie als Lemma vermutlich folgenden Sachverhalt:

$$\forall\, w, x, y, z \in \mathbb{N} : y > 0 \land x \geq y \land z > w \Rightarrow x * z > y * w$$

  In der *Prelude*-Theorie von PVS ist diese Eigenschaft bereits unter dem Namen `gt_times_gt_pos1` bewiesen.

Zentrale PVS-Kommandos: `(INDUCT)`, `(EXPAND)`, `(LIFT-IF)`, `(CASE-REPLACE)`, `(LEMMA)`.