

## Praktikum Spezifikation und Verifikation

### Univariate Polynome als Bäume

Man kann Polynome in einer Variablen mit Integer-Koeffizienten darstellen durch

`datatype poly = Var | Const int | Add poly poly | Mul poly poly`

Dabei soll zB.  $(4x - 2)x^2 + 5$  repräsentiert werden durch

`Add (Mul (Add (Mul (Const 4) Var) (Const -2)) (Mul Var Var)) (Const 5).`

Definieren Sie eine Funktion

`consts`

`eval :: "poly ⇒ int ⇒ int"`

so dass `eval p x` der Funktionswert des Polynoms `p` an der Stelle `x` ist.

Definieren Sie ein Prädikat

`consts`

`polyeq :: "poly ⇒ poly ⇒ bool"`

so dass `polyeq p q` genau dann gilt, wenn `p` und `q` dieselbe Funktion repräsentieren.

### Univariate Polynome als Listen

Polynome werden üblicherweise in der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

geschrieben.

Definieren Sie eine Funktion

**consts**

```
mkpoly :: "int list  $\Rightarrow$  poly"
```

so dass  $mkpoly [a_0, a_1, \dots, a_n]$  dieselbe Funktion repräsentiert wie obiges  $p$ .

Definieren Sie weiterhin eine Funktion, die die Koeffizienten eines Polynoms berechnet:

**consts**

```
coeffs :: "poly  $\Rightarrow$  int list"
```

Zeigen Sie  $polyeq (mkpoly (coeffs p)) p$ .

**TIP:** Definieren Sie sich Hilfsfunktionen wie zB.

**consts**

```
plus :: "int list * int list  $\Rightarrow$  int list"
```

**TIP:** Mit  $apply (simp add: ring_eq_simps)$  können häufig arithmetische Ausdrücke und Gleichungen vereinfacht werden. Mit  $apply arith$  können einfache arithmetische subgoals gelöst werden.

## Differenzieren/Ableiten von Polynomen

Definieren Sie eine Funktion,

**consts**

```
diff :: "poly  $\Rightarrow$  poly"
```

die Polynome in Baumdarstellung differenziert, und eine andere Funktion,

**consts**

```
deriv :: "int list  $\Rightarrow$  int list"
```

die Polynome in Listendarstellung differenziert. Zeigen Sie die Korrektheit von  $deriv$  bezüglich  $diff$ , indem Sie ein geeignetes Lemma formulieren und dieses beweisen.

PS: Sie dürfen bei der Definition von  $deriv$  NICHT die Definition von  $diff$  benutzen (et vice versa).

Beweisen Sie  $polyeq (diff p) (diff (mkpoly (coeffs p)))$ .

**TIP:** Nutzen Sie den Zusammenhang zwischen  $diff$  und  $deriv$  aus. Eventuell müssen Sie dazu noch mehr Eigenschaften über  $deriv$  beweisen.

▷ **Abgabe: 4. 5. 2005**