Übungen zur Vorlesung Formale Spezifikations- und Verifikationstechniken

Prof. Dr. Klaus Madlener Blatt 7

20. Aufgabe:
Sei die Relation $\leq \subseteq \mathrm{Term}(F,V) \times \mathrm{Term}(F,V)$ definiert durch:

$$\begin{aligned}
&s \lesssim t \text{ gdw. es existiert ein Substitution } \sigma \text{ mit q}t \equiv \sigma(s)\\
&s \approx t \text{ gdw. } s \lesssim t \text{ und } t \lesssim s\\
&s < t \text{ gdw. } s \lesssim t \text{ und } s \not\approx t
\end{aligned}$$

Zeigen Sie:

1. $<$ ist strikter Anteil einer wohlfundierten Partialordnung. Auf welchen Elementen ist diese Partialordnung definiert?
2. Es gilt $s \approx t$ gdw. es existiert eine Permutation ξ mit $s \equiv \xi(t)$ (Variablenumbenennung).

21. Aufgabe:
In dieser Aufgabe geht es um eine alternative Spezifikation der ganzen Zahlen INTEGER $=$ (sig, E) mit

$$sig = (int, 0, succ, pred, add),$$
$$E = \{succ(pred(x)) = x, pred(succ(x)) = x, add(0,y) = y, add(succ(x), y) = succ(add(x,y))\}$$

1. Zeigen Sie, dass $(\mathbb{Z}, 0, +1, -1, +)$ initial in Alg(INTEGER) ist.
2. Strukturieren Sie diese Spezifikation mit Hilfe der Spezifikation INT. Zeigen Sie, dass INTEGER eine Anreicherung von INT ist.
3. Erweitern Sie INTEGER um eine Funktion Betrag, die die üblichen Eigenschaften der Betragsfunktion auf $\mathbb{Z}$ hat. Zeigen Sie, dass dies eine Anreicherung von INTEGER ist.

22. Aufgabe:
Sei $sig_1 = (\{\mathrm{NAT}, \mathrm{EVEN}\}, \{0, 1, S, f\}, \{0 :\to \mathrm{NAT}, 1 :\to \mathrm{EVEN}, S : \mathrm{NAT} \to \mathrm{NAT}, f : \mathrm{NAT} \to \mathrm{EVEN}\})$. Ferner sei die sig_1-Algebra $\mathfrak{A}_1$ gegeben durch:

$$A_{1,\mathrm{NAT}} = \mathbb{N}, A_{1,\mathrm{EVEN}} = 2\mathbb{N} \cup \{1\}, 0_{\mathfrak{A}_1} = 0, 1_{\mathfrak{A}_1} = 1, S_{\mathfrak{A}_1}(x) = x+1, f_{\mathfrak{A}_1}(x) = \begin{cases} x, & \text{falls } x \text{ gerade} \\ 1, & \text{sonst} \end{cases}$$

Zeigen Sie:

1. Es gibt keine Spezifikation $spec_1 = (sig_1, E_1)$ mit E_1 endlich, so dass $T_{spec_1} \cong \mathfrak{A}_1$.

2. Es gibt eine Spezifikation $spec_2 = (sig_2, E_2)$ mit $sig_1 \subseteq sig_2$, E_2 endlich, so dass $T_{spec_2}|_{sig_1} \cong \mathfrak{A}_1$.

23. Aufgabe:

Gegeben seien folgende Spezifikationen ELEMENT und NAT.

```
spec   ELEMENT
uses   BOOL
sorts  E
opns   eq:E,E --> Bool
vars   x,y,z: --> E
eqns   eq(x,x)=true
       eq(x,y)=eq(y,x)
       eq(x,y)=true and eq(y,z)=true implies eq(x,z)=true

spec   NAT
uses   BOOL
sorts  N
opns   0: --> N
       s: N --> N
       equal: N,N --> Bool
vars   n,m: --> N
eqns   equal(0,0) = true
       equal(0,s(n) = false
       equal(s(n),0) = false
       equal(s(n),s(m)) = equal(n,m)
```

Geben Sie eine parametrisierte Spezifikation für Mengen über ELEMENT mit den Operationen INSERT und REMOVE an und zeigen Sie:

1. Der Signaturmorphismus σ : ELEMENT $\rightarrow$ NAT gegeben durch $\sigma(\mathrm{E}) = \mathrm{N}$ und $\sigma(\mathrm{eq} = \mathrm{equal})$ ist kein Spezifikationsmorphismus.

2. $(T_{\mathrm{NAT}})|\sigma$ ist jedoch Modell von ELEMENT, d.h. es ist eine korrekte Parameterzuweisung

3. Gilt für ihre Spezifikation, dass $(T_{\mathrm{VALUE}})|_{\mathrm{NAT}} \cong T_{\mathrm{NAT}}$, d.h. ist VALUE ist eine Erweiterung von NAT? Ist es eine Anreicherung?

Abgabe: bis 12.01.2006, per EMail an Bernd Strieder