

## Temporale Logik und Zustandssysteme

### Aufgabe 9-1 Herleitungen in temporaler Prädikatenlogik

a) Es sei  $A$  eine  $\mathcal{L}_{\text{FOCTL}}$ -Formel. Welche der folgenden Formeln ist allgemeingültig?

$$\diamond\Box\forall x A \rightarrow \forall x \diamond\Box A \qquad \forall x \diamond\Box A \rightarrow \diamond\Box\forall x A$$

b) Geben Sie Herleitungen für die folgenden Formeln in  $\Sigma_{\text{FOCTL}}^b$  an. Dabei dürfen Sie das Gesetz (T15) und die Regel

$$(\text{indunless}) \quad A \rightarrow \circ C \vee \circ(A \wedge B) \vdash A \rightarrow B \text{ unless } C$$

verwenden:

$$\exists x \circ A \rightarrow \circ \exists x A \qquad \exists x (A \text{ unless } B) \rightarrow (\exists x A) \text{ unless } B$$

falls  $x$  nicht frei in  $B$  vorkommt

### Aufgabe 9-2 Programmverifikation mit Temporallogik

Diese Aufgabe gibt ein erstes Beispiel zur Programmverifikation mittels temporaler Logik: Das Programm (in Pseudo-Code)

```
read(n);
a := 0; b := 1; c := 1;
while c <= n
do a := a+1; b := b+2; c := c+b
enddo;
write(a)
```

berechnet den ganzzahligen Anteil von  $\sqrt{n}$ . Dabei zeigt Teilaufgabe b) die partielle Korrektheit, während in Teilaufgabe c) die Terminierung bewiesen wird.

Die Formalisierung ist wie folgt: Gegeben sei die Signatur  $SIG$  mit der Sorte  $NAT$ , den Konstanten  $0, 1, 2, \dots$ , den zweistelligen Funktionszeichen  $+$  und  $*$  und dem zweistelligen Prädikatszeichen  $\leq$ . Wir verwenden Infixschreibweise, schreiben  $s > t$  für  $\neg(s \leq t)$  und  $s < t$  für  $t > s$ . Es seien  $a, b, c \in \mathcal{X}^F$  und  $n \in \mathcal{X}$ , und die Formel  $I$  und die Formelmenge  $\mathcal{F}$  seien gegeben durch

$$I \equiv a = 0 \wedge b = 1 \wedge c = 1$$

$$\mathcal{F} = \{c \leq n \rightarrow a' = a + 1 \wedge b' = b + 2 \wedge c' = c + b', \\ c > n \rightarrow a' = a \wedge b' = b \wedge c' = c\}$$

Ferner bezeichne  $\mathcal{A}$  die Menge aller gültigen arithmetischen Aussagen. Zeigen Sie, dass die folgenden Formeln aus  $\mathcal{F}$  und  $\mathcal{A}$  herleitbar sind:

- $I \rightarrow \Box(b = 2 * a + 1 \wedge c = (a + 1) * (a + 1) \wedge a * a \leq n)$
- $I \rightarrow \Box(c > n \rightarrow a * a \leq n \wedge n < (a + 1) * (a + 1))$
- $I \rightarrow \Diamond(c > n)$  (Benutzen Sie das Prinzip der fundierten Ordnungen.)

