Logik, Semantik und Verifikation SS 2002: Musterlösung zum 11. Übungsblatt

Prof. Dr. Gert Smolka, Dipl.-Inform. Tim Priesnitz

Aufgabe 11.1: Schwächste Vorbedingungen (4)

(a) $W = (Z = X * Y)$

(b) $W = (X = X * Y) \models\!\!\!\mid Y = 1 \vee X = 0$

(c) $W = (X \leq Y \wedge X + Y = X * Y) \vee X > Y \models\!\!\!\mid X \leq Y \Rightarrow ((X = Y = 0) \vee (X = Y = 2))$

(d) $W = \mathit{true}$

Aufgabe 11.2: Abzählbarkeit (10)

(a) Sei M abzählbar und sei $\alpha \in \mathbb{N} \to M$ surjektiv. Die folgende Funktion $\beta \in M \to \mathbb{N}$ ist wohldefiniert und injektiv:

$$\beta(m) \overset{\text{def}}{=} \min\{n \mid \alpha(n) = m\}$$

Sei $\beta \in M \to \mathbb{N}$ injektiv. Dann ist $\alpha \in \mathbb{N} \to M$ mit $\alpha(m) = n$, falls $\beta(n) = m$ surjektiv.

(b) Die Funktion $\mathbb{N}^3 \to \mathbb{N}$ mit $(n, m, o) \mapsto 3^n 5^m 7^o$ ist injektiv (nach Eindeutigkeit der Primfaktorzerlegung). Nach (a) ist $\mathbb{N}^3$ abzählbar.

(c) Sei M abzählbar. Dann gibt es nach (a) eine injektive Funktion $M \to \mathbb{N}$. Somit ist auch jede Funktion $M' \to \mathbb{N}$ mit $M' \subseteq M$ injektiv und M' abzählbar.

(d) Besuchen Sie das Hilbertsche Hotel: Das Hilbertsche Hotel besitzt für jede natürliche Zahl ein Zimmer. Durch seine Aktraktivität ist es jedoch komplett ausgebucht. Dies ist jedoch kein Hinderungsgrund eines Besuchs; der findige Potier rotiert einfach alle Gäste nach dem folgenden Prinzip: Gast 0 bekommt Zimmer 1, Gast 1 bekommt Zimmer 2, usw. Sie bekommen das nun frei gewordene Zimmer 0.

Der Beweis: Sei M abzählbar und $X = \{x_0, \ldots, x_n\}$ disjunkt von M. Dann gibt es nach (a) eine injektive Funktion $f : M \to \mathbb{N}$. Somit ist auch die Funktion $g : M \cup X \to \mathbb{N}$ mit

$$\begin{aligned} g(x_i) &= i && \text{für } x_i \in X \\ g(m) &= i + f(m) && \text{für } m \in M \end{aligned}$$

injektiv und $M \cup X$ ist abzählbar.

(e) Durch Widerspruch mit Hilfe von Cantors Diagonalargument. Sei $\alpha \in \mathbb{N} \to \mathcal{P}(\mathbb{N})$ surjektiv. Wir betrachten nun die Menge

$$M = \{n \in \mathbb{N} \mid n \notin \alpha(n)\} \subseteq \mathcal{P}(\mathbb{N}).$$

Nun gilt für alle $n \in \mathbb{N}$, dass

$$n \in \alpha(n) \Rightarrow n \notin M.$$

Es gibt also kein n mit $\alpha(n) = M$, ein Widerspruch zur Annahme α ist surjektiv.

(f) Jede Teilmenge von $\mathbb{N} \setminus \emptyset$ ist abzählbar, also ist $\mathcal{A} = \{A \subseteq \mathbb{N} \mid A \text{abzählbar}\} = \mathcal{P}(\mathbb{N}) \setminus \emptyset$. Damit folgt die Aussage aus (d) und(e).

Aufgabe 11.3: Fragen zur Berechenbarkeit (9)

(a) $X_0 := 0$

(b) if $X_0 \geq 0$ then $X_0 := 1$ else $X_0 := 0$

(c) if $-2 \leq X_0$ then if $X_0 \leq 13$ then $X_0 := 1$ else $X_0 := 0$ else $X_0 := 0$

(d) Nein, denn jede endliche Menge ist entscheidbar (siehe (c)).

(e) Sie ist injektiv, aber nicht surjektiv.

(f) S, denn $\overline{S}$ ist nicht prüfbar (Proposition 9.5.3) und S ist prüfbar (Proposition 9.5.1).

(g) $\#G$ (siehe Satz 9.6.1 und Korollar 9.6.2).

(h) Ja, eine injektive Funktion von $\{f \in \mathbb{Z} \to \mathbb{Z}_\perp \mid f \text{ berechenbar}\}$ nach $\mathbb{N}$ ist die Funktion, die f ihre kleinste Gödelnummer zuordnet.

(i) Nur $\emptyset \subseteq \mathbb{Z}$ ist nicht abzählbar.

Aufgabe 11.4: Halteproblem (7) Durch Widerspruch analog zum Beweis von Satz 9.5.2. Sei M prüfbar. Wir zeigen, dass dann S prüfbar ist. Es gilt für alle $x \in \mathbb{Z}$:

$$x \in S \iff x \in \#Com \wedge \#(X_0 := x;\, \#^{-1}x;\, X_0 := 0) \in M$$

Sei nun p eine berechenbare Prüffunktion für M. Aus der Äquivalenz folgt, dass $f \in \mathbb{Z} \to \mathbb{Z}_\perp$ mit

$$f\,x = \text{if } x \in \#Com \text{ then } p(\#(X_0 := x;\, \#^{-1}x;\, X_0 := 0)) \text{ else } \perp$$

eine Prüffunktion für S ist. Da f berechenbar ist, ist S prüfbar— ein Widerspruch.

Aufgabe 11.5: Gödelisierung in IML (10)

(a)
```
(* Signum *)
fun sg(n)   = if n>=0 then 1 else 0
(* Betrag *)
fun abs(n)  = if n<0 then ~n else n
(* Wie oft kommt m als Teiler in n vor *)
fun nt(n,m) = if n>0 andalso n mod m = 0 then nt(n div m,m)+1 else 0
(* n^m *)
fun pow(n,m) = if m=0 then 1 else n*pow(n,m-1)

fun pair(n1,n2) = pow(2,sg(n1))*pow(3,abs(n1))*
                  pow(5,sg(n2))*pow(7,abs(n2))
fun first(n)  = (if nt(n,2)=1 then ~1 else 1)*nt(n,3)
fun second(n) = (if nt(n,5)=1 then ~1 else 1)*nt(n,7)
fun ispair(n) = (n = pair(first(n),second(n)))
```

(b)
```
fun aus(n) = ispair(n) andalso
      let val f=first(n)
          val s=second(n)
      in
          f=1 orelse
          f=2 andalso s>0 orelse
          f=3 andalso aus(first(s)) andalso aus(second(s))
      end
```

Aufgabe 11.6: Konstruktion von Prüfern in IML (10)

(a) `fun f p x = if com x then p(seq(zuw x,x)) else f p x`

(b) `fun g p x = if assn x then p(neg(all x)) else g p x`