Theoretische Informatik A
Lösungen zur Klausur vom 20. März 2010

Aufgabe 1

(a) Die Behauptung (i) trifft zu.

(b) Wir beweisen die Behauptung (i) durch vollständige Induktion über $k \in \mathbb{N}$.

Induktionsanfang $k = 0$:
Offensichtlich gilt

$$\mathrm{ES}^{3\cdot 0}(2,(2,n,0,...)) = (2,(2^{2^0},n-0,0,...)).$$

Induktionsschritt $k \to k+1$:
Sei $k+1 \leq n$. Dann gilt insbesondere $k \leq n$, und wir dürfen die Induktionsannahme verwenden:

$$\begin{aligned}
& \mathrm{ES}^{3(k+1)}(2,(2,n,0,...)) \\
= \; & \mathrm{ES}^{3}(2,(2^{2^k},n-k,0,...)) && \text{(nach Ind.-annahme)} \\
= \; & \mathrm{ES}^{2}(3,(2^{2^k},n-k,0,...)) && \text{(da } n-k \geq 1 > 0) \\
= \; & \mathrm{ES}(4,(2^{2^k}\cdot 2^{2^k},n-k,0,...)) \\
= \; & (2,(2^{2^k+2^k},n-k-1,0,...)) \\
= \; & (2,(2^{2^{k+1}},n-(k+1),0,...)),
\end{aligned}$$

womit die Behauptung bewiesen ist.

(c) Es gilt

$$\begin{aligned}
& \mathrm{ES}^{3\cdot n+2}(1,(0,n,0,0,...)) \\
= \; & \mathrm{ES}^{3\cdot n+1}(2,(2,n,0,0,...)) \\
= \; & \mathrm{ES}(2,(2^{2^n},n-n,0,...)) && \text{(nach Teil (a))} \\
= \; & (5,(2^{2^n},0,0,...))
\end{aligned}$$

Da die letztgenannte Konfiguration eine Endkonfiguration ist, ergibt sich daraus

$$\mathrm{GS}(1,(0,n,0,0,...)) = (5,(2^{2^n},0,0,...)).$$

Mit dem Flussdiagramm F aus der Aufgabenstellung erhalten wir also

$$\begin{aligned} f_M(n) &= \mathrm{AC} \circ f_F \circ \mathrm{EC}^{(1)}(n) \\ &= \mathrm{AC} \circ f_F(0, n, 0, 0, \ldots) \\ &= \mathrm{AC}(2^{2^n}, 0, 0, \ldots) \\ &= 2^{2^n} \end{aligned}$$

für alle $n \in \mathbb{N}$.

Aufgabe 2

(a) Wir beweisen Behauptung durch vollständige Induktion nach $m = \lg(w)$.

<u>$m = 0$:</u>

In diesem Fall ist $w = \varepsilon$, und mit $t := 3$ und $w' := \varepsilon$ erhalten wir durch leichte Rechnung für alle $u \in \Gamma^*$ und $c \in \Gamma$:

$$\mathrm{ES}^t\,(1, (u, c, \varepsilon)) = (5, (ucw', B, \varepsilon))\,.$$

Ferner gilt die zweite Bedingung offenbar mit $n = 0$. Also gilt die Behauptung in diesem Fall.

<u>$m \to m + 1$:</u>

Sei nun $\lg(w) = m+1$. Dann gibt es $x \in \Sigma^*$ und $d \in \Sigma$, so dass $w = dx$. Es trifft nun für alle $u \in \Gamma^*$ und $c \in \Gamma$

$$\mathrm{ES}^3\,(1, (u, c, w)) = (1, (uc, c', x))$$

zu, wobei $c' = a$ im Falle $d = a$ und $c' = B$ im Falle $d = b$ gilt. Da $\lg(x) = m$ ist, können wir jetzt die Induktionsvoraussetzung auf x anwenden, und zwar mit c' anstelle von c und uc anstelle von u. Danach existieren ein $t' \in \mathbb{N}$ und ein $\hat{w} \in \Sigma^*$ mit

$$\mathrm{ES}^{t'}\,(1, (uc, c', x)) = (5, (ucc'\hat{w}, B, \varepsilon))$$

sowie

$$\forall v \in \Sigma^*\,.\,(v \text{ Suffix von } \hat{w} \iff v \text{ Suffix von } x \text{ und } \exists n \in \mathbb{N}\,.\,v = a^n).$$

Setzen wir $t := 3 + t'$ und $w' := c'\hat{w}$, dann folgt offenbar

$$\mathrm{ES}^t\,(1, (u, c, w)) = (5, (ucw', B, \varepsilon))\,,$$

und die Gültigkeit von

$$\forall v \in \Sigma^*\,.\,(v \text{ Suffix von } w' \iff v \text{ Suffix von } w \text{ und } \exists n \in \mathbb{N}\,.\,v = a^n)$$

verifiziert man ebenfalls leicht, indem man die beiden für c' möglichen Fälle unterscheidet. Damit ist der Induktionsbeweis abgeschlossen.

(b) Es sei $w \in \Sigma^*$. Wir behaupten:

$$f_M(w) = \text{das längste Suffix von } w \text{ aus } \{a\}^*.$$

Zum Beweis verwenden wir (a). Für $u = \varepsilon$ und $c = B$ liefert die dortige Behauptung die Existenz eines $t \in \mathbb{N}$ und eines $w' \in \Gamma^*$ mit

$$\mathrm{ES}^t\,(1, (\varepsilon, B, w)) = (5, (Bw', B, \varepsilon))$$

und

$$\forall v \in \Sigma^*\,.\,(v \text{ Suffix von } w' \iff v \text{ Suffix von } w \text{ und } \exists n \in \mathbb{N}\,.\,v = a^n).$$

Sei nun v das längste Suffix von w' aus Σ^*. Dann ist v auch ein Suffix von w, hat die Form a^n für ein $n \in \mathbb{N}$ und wird gemäß Ausgabecodierung der Bandmaschinen von f_M berechnet. Sei andererseits a^k ein Suffix von w, für irgendein $k \in \mathbb{N}$. Dann ist a^k auch ein Suffix von w' und aus Σ^*. Also gilt $k \leq n$. Folglich ist a^n das längste Suffix von w aus $\{a\}^*$. Damit ist die Behauptung gezeigt.

Aufgabe 3

(a) Es sei $n \in \mathbb{N}$, $n \geq 1$, und es seien $g : \mathbb{N}^{n-1} \to \mathbb{N}$ und $h : \mathbb{N}^{n+1} \to \mathbb{N}$ Funktionen. Von der durch die beiden Gleichungen

$$\begin{array}{lcl} f(\bar{x}, 0) & = & g(\bar{x}) \\ f(\bar{x}, y+1) & = & h(\bar{x}, y, f(\bar{x}, y)) \end{array}$$

für alle $\bar{x} \in \mathbb{N}^{n-1}$ und $y \in \mathbb{N}$ eindeutig bestimmten Funktion $f : \mathbb{N}^n \to \mathbb{N}$ sagt man dann, dass sie aus g und h durch *primitive Rekursion* entsteht; f wird in diesem Falle mit $\mathrm{Prk}(g, h)$ bezeichnet: $f = \mathrm{Prk}(g, h)$.

(b) Es sei $g : \mathbb{N}^3 \to \mathbb{N}$ definiert durch

$$g(x, y, z) := |x \cdot z - y|$$

für alle $x, y, z \in \mathbb{N}$. Dann ist g berechenbar, denn

$$g = \mathrm{Sub}\left(|\cdots|, \mathrm{Sub}\left(m, \mathrm{pr}_1^{(3)}, \mathrm{pr}_3^{(3)}\right), \mathrm{pr}_2^{(3)}\right),$$

geht also durch Substitution aus bekannten berechenbaren Funktionen hervor (m bezeichnet hier die Multiplikation; s. Anhang im Klausurtext).

Ferner gilt, falls x ein Teiler von y ist,

$$t(x, y) = \frac{y}{x} = \min\{z \in \mathbb{N} \mid x \cdot z = y\} = \min\{z \in \mathbb{N} \mid |x \cdot z - y| = 0\}.$$

Andernfalls ist die Menge $\{z \in \mathbb{N} \mid x \cdot z = y\}$ leer, und dann ist $t(x, y) = \mathrm{div}$. Also gilt in jedem Falle $t(x, y) = \tilde{\mu}\,(g)\,(x, y)$, d. h., $t = \tilde{\mu}\,(g)$.

Aufgabe 4

Die genannten Theoreme sind in Kurseinheit 5 des Kurstextes als Satz 7.2.2, Satz 7.2.6 und Satz 7.2.7 zu finden.

Aufgabe 5

Nach (3) des Φ-Theorems 7.2.7 ist die charakteristische Funktion g_Φ der Menge

$$\{(i, x, t) \in \mathbb{N}^3 \mid \Phi_i(x) \leq t\}$$

berechenbar. Dann ist aber auch die durch

$$h(x) := g_\Phi(x, x, 10) \text{ für alle } x \in \mathbb{N}$$

definierte Funktion berechenbar, denn sie entsteht durch Substitution berechenbarer Funktionen in g_Φ. Offenbar gilt für alle $x \in \mathbb{N}$

$$h(x) = 1 \iff g_\Phi(x, x, 10) = 1 \iff \Phi_x(x) \leq 10 \iff$$
$$u_\Phi(x, x) \neq \mathrm{div} \text{ und } u_\Phi(x, x) \leq 10 \iff f(x) = 1.$$

Genauso zeigt man, dass

$$h(x) = 0 \iff f(x) = 0$$

für alle $x \in \mathbb{N}$ gilt. D. h., $f = h$. Damit ist f berechenbar.

Aufgabe 6

Wir wollen $K_\varphi \leq A$ zeigen, womit die Behauptung bewiesen wäre. Dazu definieren wir uns eine zweistellige Funktion $f :\subseteq \mathbb{N}^2 \to \mathbb{N}$ durch

$$f(i,j) := \begin{cases} j, & \text{falls } \varphi_i(i) \text{ existiert,} \\ \text{div} & \text{sonst,} \end{cases}$$

für alle $i, j \in \mathbb{N}$. Mit Hilfe des utm-Theorems zeigt man leicht, dass $f \in P^{(2)}$ ist. Also gibt es nach dem smn-Theorem eine Funktion $r \in R^{(1)}$, so dass

$$(*) \quad \varphi_{r(i)}(j) = f(i,j)$$

für alle $i, j \in \mathbb{N}$ gilt. Wir behaupten, dass r die gewünschte Reduktion bewerkstelligt. Sei dazu zunächst $i \in K_\varphi$. Dann erhalten wir aus $(*)$ mit $j = r(i)$

$$\varphi_{r(i)}(r(i)) = r(i),$$

also $r(i) \in A$. Nun gelte $i \notin K_\varphi$. Dann ist wegen $(*)$

$$\varphi_{r(i)}(j) = \text{div}$$

für alle $j \in \mathbb{N}$. Insbesondere gilt also nicht $\varphi_{r(i)}(r(i)) = r(i)$. D. h., $r(i) \notin A$. Demnach gilt tatsächlich $K_\varphi \leq A$. Also ist A nicht rekursiv.

Aufgabe 7

Aus $K_\varphi = (\mathbb{N} \setminus A) \cap (\mathbb{N} \setminus B)$ folgt unter Benutzung bekannter mengentheoretischer Gesetze

$$\mathbb{N} \setminus K_\varphi = \mathbb{N} \setminus ((\mathbb{N} \setminus A) \cap (\mathbb{N} \setminus B)) = (\mathbb{N} \setminus (\mathbb{N} \setminus A)) \cup (\mathbb{N} \setminus (\mathbb{N} \setminus B)) = A \cup B.$$

Wäre nun sowohl A als auch B rekursiv-aufzählbar, dann auch $A \cup B$, denn die rekursiv-aufzählbaren Teilmengen von $\mathbb{N}$ sind unter Vereinigung abgeschlossen (Satz 8.2.3). Dann wäre aber auch $\mathbb{N} \setminus K_\varphi$ rekursiv-aufzählbar, was Satz 8.3.1 des Kurstextes widerspricht. Also ist A oder B nicht rekursiv-aufzählbar.

Aufgabe 8

Es sei g wie in der Aufgabenstellung definiert, also

$$g(i) := \begin{cases} 1, & \text{falls } \varphi(i) = V, \\ \text{div} & \text{sonst,} \end{cases}$$

für alle $i \in \mathbb{N}$. Dann ist $\mathrm{Def}(g) = \{i \in \mathbb{N} \mid \varphi_i = V\}$. Damit gilt – in der in Satz 8.3.9.1 („Korrektheitsproblem") eingeführten Terminologie – $\mathrm{Def}(g) = M_V$. Wegen $V \neq d$ ist $\mathrm{Def}(g)$ also, nach dem eben zitierten Satz, nicht rekursiv-aufzählbar. Damit ist g nicht berechenbar.

Aufgabe 9

(a) Es sei $m \in \mathbb{N}$. Dann lässt sich m wie folgt darstellen:

$$m = \frac{m-0}{1}\,.$$

Also gilt $m = \nu\langle m, 0, 0\rangle$. Damit ist ν surjektiv, also eine Nummerierung von $\mathbb{N}$.

(b) Zuerst zeigen wir $\nu \leq \mathrm{id}_{\mathbb{N}}$. Dazu definieren wir $f :\subseteq \mathbb{N} \to \mathbb{N}$ durch

$$f\langle i, j, k\rangle := \begin{cases} q(i-j, k+1), & \text{falls } i \geq j \text{ und } r(i-j, k+1) = 0, \\ \text{div} & \text{sonst,} \end{cases}$$

für alle $\langle i, j, k\rangle \in \mathbb{N}$. Die Funktion f ist u. a. wegen Satz 4.2.2 berechenbar; q und r sind dabei die Funktionen aus dem Anhang im Klausurtext (s. 10.). (Wir verzichten hier darauf, explizit das Flussdiagramm einer verallgemeinerten Registermaschine mit berechenbaren Funktionen und Tests anzugeben, die f berechnet.) Offenbar gilt nun

$$\nu\langle i, j, k\rangle = f\langle i, j, k\rangle = \mathrm{id}_{\mathbb{N}}\,(f\langle i, j, k\rangle)$$

für alle $\langle i,j,k\rangle \in \mathrm{Def}(\nu)$, denn $\nu_{\mathbb{Q}}\langle i,j,k\rangle \in \mathbb{N}$ trifft genau zu, wenn $i \geq j$ und $r(i-j,k+1) = 0$ gilt, und in diesem Falle ist $\nu_{\mathbb{Q}}\langle i,j,k\rangle = q(i-j,k+1)$. Damit ist $\nu \leq \mathrm{id}_{\mathbb{N}}$ gezeigt.

Nun zur umgekehrten Reduzierbarkeit, die leichter zu zeigen ist. Wir definieren $g : \mathbb{N} \to \mathbb{N}$ durch

$$g(n) := \langle n,0,0\rangle \text{ für alle } n \in \mathbb{N}.$$

Wiederum nach Satz 4.2.2 (u. a.) ist g berechenbar, und es gilt

$$\mathrm{id}_{\mathbb{N}}(n) = n = \frac{n-0}{1} = \nu_{\mathbb{Q}}\langle n,0,0\rangle = \nu\langle n,0,0\rangle = \nu\left(g(n)\right)$$

für alle $n \in \mathbb{N}$. Dies beweist $\mathrm{id}_{\mathbb{N}} \leq \nu$.

Aufgabe 10

1. (a) Richtig.
   (b) Falsch.
   (c) Richtig.
   (d) Richtig.
   (e) Falsch.
2. (f) Richtig.
   (g) Falsch.
   (h) Falsch.
   (i) Falsch.
   (j) Richtig.
3. (k) Falsch.
   (l) Falsch.