Einführung in die Theoretische Informatik B
Lösungsvorschläge zur
Klausur am 31. Juli 2004
Sommersemester 2004

Aufgabe 1 (von oben nach unten)

1) korrekt, falsch, korrekt, korrekt, korrekt, falsch, korrekt
2) dkf, dkf, nicht dkf, nicht dkf
3) regulär, nicht regulär, regulär
4) korrekt, korrekt, korrekt, falsch, korrekt, falsch
5) korrekt, korrekt, falsch, korrekt, falsch
6) korrekt, korrekt, korrekt, nicht korrekt, korrekt

Aufgabe 2

(a) Siehe Def. 4.1.3

(b) Siehe Def. 3.5.1

(c) Siehe Def. 4.3.5

(d) Siehe Def. 4.3.5

(e) Siehe Def. 7.1.1

(f) Siehe Def. 8.3.2

Aufgabe 3

(1) Da $f(n) > n$ für alle $n \in \mathbb{N}$ gilt, folgt:
$(f \circ g)(n) = f(g(n)) > g(n)$ für alle $n \in \mathbb{N}$.

zu a) Mit (1) folgt für alle $n \in \mathbb{N}$: $(g + (f \circ g))(n) = g(n) + (f \circ g)(n)$
$< 2 \cdot (f \circ g)(n)$,

somit folgt $g + f \circ g \in O(f \circ g)$

zu b) Da f und g zeitkonstruierbar sind, gibt es TM M_1, M_2 mit
$f_{M_1}(\emptyset^n) = \emptyset^{f(n)}, f_{M_2}(\emptyset^n) = \emptyset^{g(n)}, \tilde{t}_{M_1} \in O(f)$ sowie $\tilde{t}_{M_2} \in O(g)$

Betrachte folgende TM M:
Eingabe: $\emptyset^n$

(1) Berechne $\emptyset^{g(n)}$ mit M_2.

(2) Berechne $\emptyset^{f(g(n))}$ mit M_1 und dem Ergebnis aus (1).

(3) Gebe $\emptyset^{f(g(n))}$ aus.

Offensichtlich gilt $f_M(\emptyset^n) = \emptyset^{f(g(n))}$.
Zeitanalyse:

(1) $O(g)$

(2) $O(f \circ g)$

(3) $O(f \circ g)$

Insgesamt $O(g + f \circ g)$. Mit (a) folgt $O(g + f \circ g) = O(f \circ g)$.
Somit ist $f \circ g$ zeitkonstruierbar.

Aufgabe 4

(a) Es ist zu zeigen, dass aus $L \in \mathrm{P}$ und $M \leq_{LIN} L$ folgt, dass $M \in \mathrm{P}$ gilt.
Sei also $L \in \mathrm{P}$ via TM K und gelte $M \leq_{LIN} L$ via f. Betrachte folgende TM N:

Eingabe x.

(1) Berechne $f(x)$

(2) Entscheide $f(x) \in L$ mittels K und akzeptiere genau dann, wenn K akzeptiert.

Es gilt $L_N = M$, da $x \in L_N \Leftrightarrow f(x) \in L \Leftrightarrow x \in M$ gilt.

Zeitanalyse:

(1) $O(|x|)$

(2) $O(|f(x)|^k)$ für ein $k \in \mathbb{N}$.

Da $f \in \text{FZEIT}(n)$ gilt $|f(x)| \in O(|x|)$. Somit insgesamt $O(|x|^k)$ Schritte, also $M \in \text{P}$.

(b) Angenommen, es gäbe eine vollständige Sprache L für P bzgl. $\leq_{LIN}$. Da L P-vollständig ist, gilt:

(a) $L' \leq_{LIN} L$ für alle $L' \in \text{P}$ und

(b) $L \in \text{P}$.

Wegen (b) existiert ein k, so dass $L \in \text{ZEIT}(n^k)$. Mit (a) folgt daraus, dass $\text{P} \subseteq \text{ZEIT}(n^{k+1})$. Dies ist ein Widerspruch zu den Zeithierarchiesätzen, da aus ihnen $\text{ZEIT}(n^{k+1}) \subsetneq \text{P}$ folgt.

Aufgabe 5

(i) Die Reduktion sieht wie folgt aus:

$$f(x) = \begin{cases} d(a_1)\sharp \ldots \sharp d(a_m)\sharp d(0)\sharp d(N), & \text{falls } x = d(N)\sharp d(a_1)\sharp \ldots \sharp d(a_m) \\ d(10)\sharp d(0)\sharp d(0), & \text{sonst} \end{cases}$$

$f \in \text{FPTIME}$ ist offensichtlich.

Es bleibt $x \in \text{RUCKSACK} \Leftrightarrow f(x) \in \text{DOPPELT}$ zu zeigen.

„$\Rightarrow$" Sei $x \in \text{RUCKSACK}$, $x = d(N)\sharp d(a_1)\sharp \ldots \sharp d(a_m)$. Dann gibt es $I \subseteq \{1, \ldots, m\}$ mit $\sum_{i \in I} a_i = N$. Offensichtlich gilt $\emptyset \cap I = \emptyset$ und $0 \leq N$ für alle $N \in \mathbb{N}$. Somit ist $f(x) \in \text{DOPPELT}$.

„$\Leftarrow$" Sei also $f(x) \in \text{DOPPELT}$ und $f(x) = d(a_1)\sharp \ldots \sharp d(a_m)\sharp d(0)\sharp d(N)$. Dann folgt dass es I, J gibt mit $\sum_{i \in I} a_i = 0$ und $\sum_{i \in J} a_i = N$ und $I \cap J = \emptyset$. Somit ist, da $\sum_{i \in J} a_i = N$, also $x \in \text{RUCKSACK}$.

(ii) DOPPELT $\in$ NP wie man durch die Angabe einer nichtdeterminierten Turingmaschine, die DOPPELT in Polynomialzeit erkennt, leicht zeigt. Da RUCKSACK NP-vollständig ist, gilt mit (i) für alle $L \in \text{NP}$, dass $L \leq_{pol} \text{RUCKSACK} \leq_{pol} \text{DOPPELT}$. Also ist DOPPELT NP-hart und somit auch NP-vollständig.

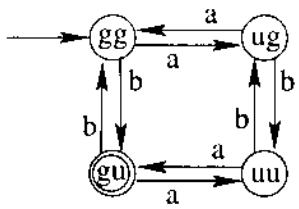
Aufgabe 6

(a) (i) $\alpha_1 = a \cup (a \cup b)^* b$

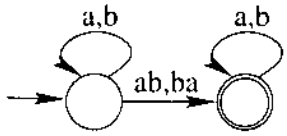
(ii) $\alpha_2 = a(a \cup b)^* b$

(iii) $\alpha_3 = (a \cup b)^* a (a \cup b)^* a (a \cup b)^*$

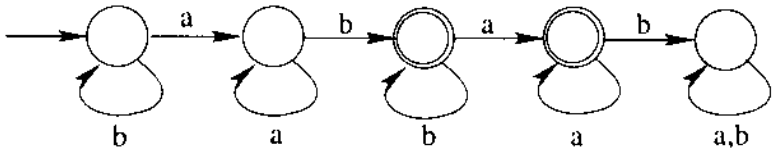
(b) (i)



(ii)



(c)



(d) Es gilt $\{w \in \{a,b\} \mid w \text{ enthält das Teilwort } ab\} = \emptyset$. Somit ist $G = (\{S\}, \{a,b\}, \emptyset, S)$ eine rechtslineare Grammatik, die die Aufgabenstellung erfüllt.

Eigentlich sollte $\{w \in \{a,b\}^* \mid w \text{ enthält das Teilwort } ab\}$ erzeugt werden. Für diese Sprache ist das folgende G eine mögliche Lösung.

$$\begin{aligned} R = \{ \; & S \to aS|bS|aA, \\ & A \to bB, \\ & B \to aB|bB|\varepsilon\} \\ G = (\{S,A,B\}, & \{a,b\}, R, S) \end{aligned}$$

Aufgabe 7

Angenommen, L sei kontextfrei. Sei p die Zahl aus dem Pumpinglemma. Wir wählen $z := a^p b^p c^{2p} d^{2p}$. Dann ist $z \in L$ und $\lg(z) \geq p$. Seien $u, v, w, x, z \in \{a,b,c,d\}^*$, so dass $z = uvwxy$, $vx \neq \varepsilon$ und $\lg(vwx) \leq p$. Dann sind folgende Fälle möglich:

(i) $vwx \in \{a,b\}^*$: Sei $z' := uv^0wx^0y$. Dann gilt $\sharp_a(z') + \sharp_b(z') < 2p$ und $\sharp_c(z') + \sharp_d(z') = 4p$. Somit $z' \notin L$.

(ii) $vwx \in \{b,c\}^*$: Sei $z' := uv^0wx^0y$. Dann gilt $\sharp_b(z') + \sharp_c(z') < 3p$ und $\sharp_a(z') + \sharp_d(z') = 3p$. Somit $z' \notin L$.

(iii) $vwx \in \{c,d\}^*$: $z' := uv^0wx^0y \Rightarrow \sharp_c(z') + \sharp_d(z') < 4p$ und $\sharp_a(z') + \sharp_b(z') = 2p$. Somit $z' \notin L$.

Widerspruch.

Somit ist L nicht kontextfrei.

Aufgabe 8

(a) $n = 0$ In 0 Schritten kann nur S aus S abgeleitet werden. Somit gilt die Behauptung für $n = 0$.

$n > 0$ $S \xrightarrow{n+1} w \Rightarrow \exists \beta.\ S \xrightarrow{n} \beta \xrightarrow{1} w$

Da $\beta \xrightarrow{1} w$, gibt es $\beta_1, \beta_2 \in (\Sigma \cup \Pi)^*$ mit $\beta = \beta_1 S \beta_2$. Nach IV gilt $\beta \in L$. Es sind drei Fälle möglich:

1.) $w = \beta_1\beta_2$. Es ist $\sharp_<(w) = \sharp_<(\beta) = \sharp_>(\beta) = \sharp_>(w)$
Da in β für jedes Präfix u die Aussage $\sharp_<(u) \geq \sharp_>(u)$ gilt, gilt dies auch für w, da sich β und w nur um ein S unterscheiden.

2.) $w = \beta_1 aSb\beta_2$. $\sharp_<(w) = \sharp_<(\beta) + 1 = \sharp_>(\beta) + 1 = \sharp_>(w)$.
Die Präfixeigenschaft gilt offensichtlich.

3.) $w = \beta_1 SS\beta_2$. $\sharp_<(w) = \sharp_<(\beta) = \sharp_>(\beta) = \sharp_>(w)$. Die Präfixeigenschaft gilt, da sich β und w nur um SS unterscheiden.

(b) Sei $x \in L(G) \Rightarrow \exists n \in \mathbb{N}.\ S \xrightarrow{n} x$. Somit folgt mit (a) direkt $x \in L$, da $x \in \{<,>\}^*$.

(c) Wir zeigen mit Induktion.

Für alle $w \in L$ mit $lg(w) = n$ gilt $w \in L(G)$. $(**)$

$n = 0$: Es ist $\varepsilon \in L$ und $\varepsilon \in L(G)$, also gilt $(**)$ für $n = 0$.

$n > 0$: Sei $w \in L$ und $lg(w) = n + 1$. Mit $(*)$ gilt, dass für w einer der zwei folgenden Fälle gilt:

(1) $w =< u >$ mit $u \in L$
oder

(2) $w = uv$ mit $v \neq w$ und $u = w$ und $u, v \in L$

zu (1) $lg(u) < lg(w)$. Somit ist die Induktionsvoraussetzung auf u anwendbar. Also $\exists n.\ S \xrightarrow{n} u$.
Somit $S \rightarrow < S > \xrightarrow{n} < u >= w$. Also $w \in L(G)$.

zu (2) $lg(u) < lg(w)$ und $lg(v) < lg(w)$. Somit $\exists n_1.\ S \xrightarrow{n_1} u$ und $\exists n_2.\ S \xrightarrow{n_2} v$. Daraus folgt $S \rightarrow SS \xrightarrow{n_1} uS \xrightarrow{n_2} uv = w$. Also $w \in L(G)$.

(d) Für $w = \varepsilon$ ist nichts zu zeigen. Sei also $w \in L$ und $lg(w) > 0$.
Es sei u das kürzeste Präfix $\neq \varepsilon$ von w mit $\sharp_<(u) = \sharp_>(u)$.
Ist $u = w$, dann gilt $w =< u' >$ mit $u' \in \{<,>\}^*$. Für u' gilt $\sharp_<(u') = \sharp_>(u')$.
Angenommen es existiert ein echtes Präfix v von u' mit $\sharp_<(v) < \sharp_>(v)$.
Dann folgt $\sharp_<(v) \leq \sharp_>(v)$ und somit $\sharp_<(v) = \sharp_>(v)$. Widerspruch.

Ist $u \neq w$, dann folgt $u \in L$ und $w = uu'$ mit $\sharp_<(u') = \sharp_>(u')$.
Gäbe es ein Präfix u'' von u' mit $\sharp_<(u'') < \sharp_>(u'')$, dann gilt auch $\sharp_<(uu'') < \sharp_>(uu'')$. Somit $u'' \in L$.