Universität Siegen
Lehrstuhl Theoretische Informatik
Markus Lohrey

Übungsblatt 3

Aufgabe 1

Postsches Korrespondenzproblem (PCP)
Gegeben: Eine Folge von Paaren $(s_1, t_1), \ldots, (s_k, t_k)$ mit $k \geq 0, s_i, t_i \in \{0,1\}^*$ $(1 \leq i \leq k)$.
Frage: Existieren Indizes $i_1, \ldots, i_m \in \{1, \ldots, k\}$ $(m \geq 1)$ mit $s_{i_1} \cdots s_{i_m} = t_{i_1} \cdots t_{i_m}$?

Seien e ein nullstelliges Funktionssymbol, f_0 und f_1 einstellige Funktionssymbole und P ein zweistelliges Relationssymbol. Zu einem String $z = c_1 \ldots c_\ell \in \{0,1\}^\ell$ $(\ell \geq 0)$ und einem Term t schreiben wir $f_z(t)$ für den Term $f_{c_\ell}(\ldots(f_{c_1}(t))\ldots)$. Seien

$$\phi_1 = \bigwedge_{i=1}^{k} P(f_{s_i}(e), f_{t_i}(e)),$$

$$\phi_2 = \forall v \forall w (P(v,w) \to \bigwedge_{i=1}^{k} P(f_{s_i}(v), f_{t_i}(w))),$$

$$\phi_3 = \exists z (P(z,z))$$

und sei $\phi = \phi_1 \wedge \phi_2 \to \phi_3$. Zeigen Sie, dass ϕ genau dann allgemeingültig ist, wenn das Postsche Korrespondenzproblem eine Lösung hat.

Lösung
Für die eine Richtung nehmen wir an, dass ϕ allgemeingültig ist. Die Idee ist nun, eine Struktur $\mathcal{A}$ zu definieren, die uns die Existenz einer Lösung liefert. Dazu definieren wir $\mathcal{U}_\mathcal{A} = \{0,1\}^*$, $e^\mathcal{A} = \varepsilon$, $f_0^\mathcal{A}(s) = s0$, $f_1^\mathcal{A}(s) = s1$ und

$$P^\mathcal{A} = \{(s,t) \mid \exists (i_1, \ldots, i_m) \in \mathbb{N}^m . s = s_{i_1} \ldots s_{i_m} \wedge t = t_{i_1} \ldots t_{i_m}\}.$$

Dementsprechend ist $e^\mathcal{A}$ das leere Wort ε und mit $f_0^\mathcal{A}$, $f_1^\mathcal{A}$ (und dementsprechend $f_w^\mathcal{A}$ für $w \in \{0,1\}^*$) werden Wörter konkateniert (zum Beispiel ist $f_v^\mathcal{A}(u) = uv$). Für ein Paar $(s,t) \in \{0,1\}^* \times \{0,1\}^*$ mit $(s,t) \in P^\mathcal{A}$ gilt, dass s und t sich aus den s_i's bzw. t_i's mit den gleichen Indizes zusammensetzen lassen. Da ϕ allgemeingültig ist, gilt auch $\mathcal{A} \models \phi$. Wenn wir zeigen, dass auch $\mathcal{A} \models \phi_1 \wedge \phi_2$, so können wir schließen, dass $\mathcal{A} \models \phi_3$, d.h. es gibt eine Lösung für das PCP, denn z lässt sich sowohl aus den s_i's als auch aus den t_i's mit den gleichen Indizes bilden. Zunächst gilt $\mathcal{A} \models \phi_1$, denn $f_{s_i}^\mathcal{A}(e^\mathcal{A}) = s_i$, $f_{t_i}^\mathcal{A}(e^\mathcal{A}) = t_i$ und außerdem $(s_i, t_i) \in P^\mathcal{A}$ für jedes $1 \leq i \leq k$. Nun zeigen wir $\mathcal{A} \models \phi_2$: Seien $s, t \in \{0,1\}^*$ mit $(s,t) \in P^\mathcal{A}$. Daraus folgt, dass es eine Folge von Indizes $(i_1, \ldots, i_m)$ gibt mit $s = s_{i_1} \ldots s_{i_m}$ und $t = t_{i_1} \ldots t_{i_m}$. Sei $1 \leq j \leq k$. Wir haben zu zeigen, dass $(f_{s_j}^\mathcal{A}(s), f_{t_j}^\mathcal{A}(t)) \in P^\mathcal{A}$. Dies gilt, weil es Indizes $(i_1, \ldots, i_m, j)$ gibt mit $f_{s_j}^\mathcal{A}(s) = s_{i_1} \ldots s_{i_m} s_j$ und $f_{t_j}^\mathcal{A}(t) = t_{i_1} \ldots t_{i_m} t_j$.

Für die andere Richtung zeigen wir nun, dass $\mathcal{A} \models \phi$ für *jedes* $\mathcal{A}$, wenn das PCP eine Lösung hat. Sei $(i_1, \ldots, i_m)$ diese Lösung. Im Fall $\mathcal{A} \not\models \phi_1$ oder $\mathcal{A} \not\models \phi_2$ gilt $\mathcal{A} \models \phi$ trivialerweise. Gelte also nun $\mathcal{A} \models \phi_1$ und $\mathcal{A} \models \phi_2$, also müssen wir zeigen, dass auch $\mathcal{A} \models \phi_3$. Sei $\psi\colon \{0,1\}^* \to \mathcal{U}_\mathcal{A}$ definiert als $\psi(\varepsilon) = e^\mathcal{A}$, $\psi(s0) = f_0^\mathcal{A}(\psi(s))$ und schließlich $\psi(s1) = f_1^\mathcal{A}(\psi(s))$. Zunächst gilt wegen $\mathcal{A} \models \phi_1$, dass $(\psi(s_i), \psi(t_i)) \in P^\mathcal{A}$ für alle $1 \leq i \leq k$. Insbesondere gilt also $(\psi(s_{i_1}), \psi(t_{i_1})) \in P^\mathcal{A}$. Wir zeigen nun per Induktion, dass auch $(\psi(s_{i_1} \ldots s_{i_m}), \psi(t_{i_1} \ldots t_{i_m})) \in P^\mathcal{A}$. Gelte $(\psi(s_{i_1} \ldots s_{i_\ell}), \psi(t_{i_1} \ldots t_{i_\ell})) \in P^\mathcal{A}$ für $1 \leq \ell < m$. Wegen $\mathcal{A} \models \phi_1$ gilt $(\psi(s_{i_{\ell+1}}), \psi(t_{i_{\ell+1}})) \in P^\mathcal{A}$. Nach Definition von ψ gilt für alle $v, w \in \{0,1\}^*$, dass $\psi(vw) = f_w^\mathcal{A}(\psi(v))$. Insbesondere gilt also auch $\psi(s_{i_1} \ldots s_{i_{\ell+1}}) = f_{s_{i_{\ell+1}}}^\mathcal{A}(\psi(s_{i_1} \ldots s_{i_\ell}))$ und $\psi(t_{i_1} \ldots t_{i_{\ell+1}}) = f_{t_{i_{\ell+1}}}^\mathcal{A}(\psi(t_{i_1} \ldots t_{i_\ell}))$. Wegen $\mathcal{A} \models \phi_2$ können wir also schließen, dass $(\psi(s_{i_1} \ldots s_{i_\ell+1}), \psi(t_{i_1} \ldots t_{i_{\ell+1}})) \in P^\mathcal{A}$, was die Induktion zeigt. Da $(\psi(s_{i_1} \ldots s_{i_m}), \psi(t_{i_1} \ldots t_{i_m}) \in P^\mathcal{A}$ und da $s_{i_1} \ldots s_{i_m} = t_{i_1} \ldots t_{i_m}$, weil $(i_1, \ldots, i_m)$ eine Lösung des PCP ist, erhalten wir, dass $\mathcal{A} \models \phi_3$ und somit $\mathcal{A} \models \phi$.