Semantik und Programmverifikation

Prof. Dr. Christoph Walther / Simon Siegler
Technische Universität Darmstadt — Wintersemester 2008/09

Übungsblatt mit Lösungsvorschlag 2

Aufgabe 2.1 (Konfluente Relationen)

Sei M eine Menge und $\rightarrow \subset M \times M$. Dann heißt die Relation $\rightarrow$ einseitig konfluent gdw.

$$\leftarrow \circ \rightarrow^* \subset \rightarrow^* \circ {}^*\leftarrow.$$

Beweisen oder widerlegen Sie die folgenden Behauptungen:

(a) Wenn $\rightarrow$ konfluent, dann ist $\rightarrow$ einseitig-konfluent.

Lösungsvorschlag:

Die Aussage ist wahr.

Annahme: $\rightarrow$ ist konfluent, also für alle $q, s, t \in M$: wenn es ein $n \in \mathbb{N}$ mit $q \rightarrow^n s$ gibt und $q \rightarrow^* t$, dann gibt es ein $r \in M$ mit $s \rightarrow^* r$ und $t \rightarrow^* r$.

Herausziehen des Existenzquantors für n ergibt: Für alle $q, s, t \in M$, $n \in \mathbb{N}$: wenn $q \rightarrow^n s$ und $q \rightarrow^* t$, dann gibt es ein $r \in M$ mit $s \rightarrow^* r$ und $t \rightarrow^* r$.

Instantiieren wir n mit 1, ergibt sich gerade die Definition der einseitigen Konfluenz.

(b) Wenn $\rightarrow$ einseitig-konfluent, dann ist $\rightarrow$ konfluent.

Lösungsvorschlag:

Die Aussage ist wahr.

Annahme: sei $\rightarrow$ einseitig konfluent, also für alle $q, s, t \in M$: wenn $q \rightarrow^1 s$ und $q \rightarrow^* t$, dann gibt es ein $r \in M$ mit $s \rightarrow^* r$ und $t \rightarrow^* r$.

Zu zeigen (vgl. (a)). Für alle $q, s, t \in M$, $n \in \mathbb{N}$: wenn $q \rightarrow^n s$ und $q \rightarrow^* t$, dann gibt es ein $r \in M$ mit $s \rightarrow^* r$ und $t \rightarrow^* r$. Dies nennen wir $A(n)$.

Wir zeigen $A(n)$ durch Induktion über n.

Basisfall $A(0)$**:** Wir nehmen an, (1.) $q \rightarrow^0 s$ (2.) $q \rightarrow^* t$. Zu zeigen: Es gibt ein $r \in M$ mit $s \rightarrow^* r$ und $t \rightarrow^* r$.

Wir wählen $r = t$. Denn wegen (1.) folgt $q = s$ und mit (2.) folgt $s \rightarrow^* t$. Und wegen der Reflexivität von $\rightarrow^*$ gilt auch $t \rightarrow^* t$. (Die Voraussetzung der einseitigen Konfluenz wurde nicht benötigt.)

Schrittfall $A(n) \Rightarrow A(n+1)$**:** Wir nehmen an: (IH) $A(n)$ (1.) $q \rightarrow^{n+1} s$ (2.) $q \rightarrow^* t$, Zu zeigen: $t \rightarrow^* r$ und $s \rightarrow^* r$ für ein $r \in M$.

Aus (1.) folgt (3.) $q \rightarrow^n s'$ und (4.) $s' \rightarrow^1 s$ für ein $s' \in M$. Aus (3.) und (2.) folgt mit (IH), dass es ein $r' \in M$ mit (5.) $s' \rightarrow^* r'$ und (6.) $t \rightarrow^* r'$ gibt. Aus (4.) und (5.) folgt mit der einseitigen Konfluenz, dass es ein $r'' \in M$ mit (7.) $s \rightarrow^* r''$ und (8.) $r' \rightarrow^* r''$ gibt. Wir wählen $r = r''$. Mit der Transitivität von $\rightarrow^*$, (6.) und (8.) folgt dann $t \rightarrow^* r$, mit (7.) $s \rightarrow^* r$.

Aufgabe 2.2 (Newmann-Lemma)

Beweisen Sie folgende Aussage (vgl. Satz 1.5.1):

Sei $\rightarrow \subset M \times M$ eine *fundierte* Relation. Dann ist $\rightarrow$ konfluent gdw. $\rightarrow$ lokal konfluent ist.

Lösungsvorschlag:

Konfluenz impliziert lokale Konfluenz, also ist nur die andere Richtung zu zeigen. Sei also $\rightarrow \subset M \times M$ eine fundierte und lokal konfluente Relation. Wir zeigen durch Noethersche Induktion die folgende Aussage:

$$\forall q \in M.\ q \rightarrow^* s \wedge q \rightarrow^* t \implies \exists r \in M.\ s \rightarrow^* r \wedge t \rightarrow^* r$$

Induktionsanfang: Sei $q \in M$ ein $\rightarrow$-minimales Element. Mit $q \rightarrow^* s \wedge q \rightarrow^* t$ folgt $q = s = t$ und damit gilt $s \rightarrow^* q \wedge t \rightarrow^* q$

Induktionsschritt: Da $q \in M$ nicht minimal ist, folgt aus $q \rightarrow^* s \wedge q \rightarrow^* t$, dass es $s', t' \in M$ gibt, so dass $q \rightarrow s' \rightarrow^* s \wedge q \rightarrow t' \rightarrow^* t$. Mit der lokalen Konfluenz von $\rightarrow$ gibt es dann ein $r' \in M$ mit $s' \rightarrow^* r' \wedge t' \rightarrow^* r'$.

Aus $s' \rightarrow^* r' \wedge s' \rightarrow^* s$ folgt nach Induktionshypothese $\exists r_s \in M.\ r' \rightarrow^* r_s \wedge s \rightarrow^* r_s$ und aus $t' \rightarrow^* r' \wedge t' \rightarrow^* t$ folgt $\exists r_t \in M.\ r' \rightarrow^* r_t \wedge t \rightarrow^* r_t$. Auch auf $r' \rightarrow^* r_s \wedge r' \rightarrow^* r_t$ ist die Induktionshypothese anwendbar und man erhält $\exists r \in M.\ r_s \rightarrow^* r \wedge r_t \rightarrow^* r$. Also gilt $s \rightarrow^* r_s \rightarrow^* r \wedge t \rightarrow^* r_t \rightarrow^* r$ und somit auch die Konfluenz.

Aufgabe 2.3 (Noether-Induktion)

Beweisen Sie unter Verwendung Noetherscher Induktion das folgende Substitutionslemma für Terme (vgl. Satz 1.2.1.i):

Sei $\sigma = \{x_i/t_i \mid 1 \leq i \leq n\}$ eine Substitution über Σ und $\mathcal{V}$. Dann gilt für alle Terme $r \in \mathcal{T}(\Sigma, \mathcal{V})$ und für alle Σ–Interpretationen (A, a)

$$a(\sigma(r)) = (a\,[x_1/a(t_1), \ldots, x_n/a(t_n)])(r).$$

Zur Erinnerung: Dabei bezeichne $a[x_1/c_1, \ldots, x_n/c_n]$ eine A-Variablenbelegung a mit

$$a[x_1/c_1, \ldots, x_n/c_n](x_i) = c_i$$

für alle x_i mit $1 \leq i \leq n$ und c_i Trägerelement von A und

$$a[x_1/c_1, \ldots, x_n/c_n](y) = a(y)$$

sonst (vgl. Def. 1.2.1)

Lösungsvorschlag:

Beweis durch strukturelle Induktion über r:

Basisfall $r \in \mathcal{V}$ **und** $r \in \mathrm{dom}(\sigma)$**:** $\Rightarrow r = x_i$ für ein i mit $1 \leq i \leq n \Rightarrow a(\sigma(r)) = a(\sigma(x_i)) = a(t_i) = a[x_1/a(t_1), \ldots, x_n/a(t_n)](x_i) = a[x_1/a(t_1), \ldots, x_n/a(t_n)](r)$

Basisfall $r \in \mathcal{V}$ **und** $r \notin \mathrm{dom}(\sigma)$**:** $\Rightarrow a(\sigma(r)) = a(r) = a[x_1/a(t_1), \ldots, x_n/a(t_n)](r)$

Basisfall $r \in (\Sigma_{\lambda,s})_{s \in \mathcal{S}}$**:** $\Rightarrow a(\sigma(r)) = \alpha_r = a[x_1/a(t_1), \ldots, x_n/a(t_n)](r)$

Schrittfall $r = f(r_1, \ldots, r_m)$ **mit** $f \in \Sigma_{w,s}, w \in \mathcal{S}^+, s \in \mathcal{S}, r_1 \ldots r_m \in \mathcal{T}(\Sigma, \mathcal{V})_w$**:** Wir haben die m Induktionshypothesen (IH) $a(\sigma(r_i)) = (a\,[x_1/a(t_1), \ldots, x_n/a(t_n)])(r_i), 1 \leq i \leq m$

$a(\sigma(r))$	Fall
$= a(\sigma(f(r_1, \ldots, r_m)))$	Def. 1.1.6: Substitution
$= a(f(\sigma(r_1), \ldots, \sigma(r_m)))$	Def 1.2.1: Auswertungsfunktion
$= \alpha_f(a(\sigma(r_1)), \ldots, a(\sigma(r_m)))$	m Induktionshypothesen
$= \alpha_f(a[x_1/a(t_1), \ldots, x_n/a(t_n)](r_1), \ldots, a[x_1/a(t_1), \ldots, x_n/a(t_n)](r_m)$	Def 1.2.1: Auswertungsfunktion
$= a[x_1/a(t_1), \ldots, x_n/a(t_n)](f(r_1, \ldots, r_m))$	Fall
$= a[x_1/a(t_1), \ldots, x_n/a(t_n)](r)$	