Bemerkung zum Standard-Datenmodell

Sei spec $=$ (sig, R) zulässige Spezifikation über
sig $= (S, C, F, \alpha)$ und $V = V^C$.

1. Bemerkung

Sei spec eine positiv-bedingte Spezifikation und seien alle $f \in F - C$ total definiert (d. h., für alle $t \in$ Term(F) gibt es $t' \in$ Term(C) mit $t =_R t'$).
Dann ist in $\mathcal{M}_e^C$ jedes $f^{\mathcal{M}_e^C}$ total definiert und $\mathcal{M}_e^C = \mathcal{M}$ ist isomorph zum initialen Modell $\mathcal{I} = \mathcal{I}$(spec) von früher.

2. Bemerkung Sei $t, t_1, t_2 \in$ Term(F)

Gilt $\mathcal{M} \models \mathrm{def}(t)$, so gilt $\mathcal{A} \models \mathrm{def}(t)$ für alle $\mathcal{A} \in$ DMod(spec).
Gilt $\mathcal{M} \not\models \mathrm{def}(t)$, so kann $\mathcal{A} \models \mathrm{def}(t)$ für ein $\mathcal{A} \in$ DMod(spec) gelten.
Gilt $\mathcal{M} \models t_1 = t_2$, so gilt $\mathcal{A} \models t_1 = t_2$ für alle $\mathcal{A} \in$ DMod(spec).
Gilt $\mathcal{M} \not\models t_1 = t_2$, so kann $\mathcal{A} \models t_1 = t_2$ für ein $\mathcal{A} \in$ DMod(spec) gelten.
Aber: Gilt $\mathcal{M} \models \mathrm{def}(t_1) \wedge \mathrm{def}(t_2)$, so gilt $\mathcal{M} \models t_1 = t_2$ gdw DMod(spec) $\models t_1 = t_2$.

3. Bemerkung

Ziel ist es, für Klauseln D zu zeigen DMod(spec) $\models D$. Die 2. Bemerkung zeigt, dass es reicht $\mathcal{M} \models D$ zu zeigen, falls $\mathcal{M} \models \mathrm{def}(t_1) \wedge \mathrm{def}(t_2)$ gilt für alle negativen Literale $t_1 \neq t_2$ in D. Also: $\mathcal{M} = \mathcal{M}$(spec) spielt eine ähnliche Rolle wie früher $\mathcal{I} = \mathcal{I}$(spec).

Ergebnisse zum Standard-Datenmodell

Sei sig $= (S, C, F, \alpha)$, spec $=$ (sig, R) zulässig,
$\mathcal{M} = \mathcal{M}$(spec).

Lemma 4.5

Für alle $t_1, t_2 \in$ Term(F, V^G) gilt

$$t_1 =_R t_2 \ \mathrm{gdw}\ \text{DMod(spec)} \models t_1 = t_2.$$

Satz 4.1.

Sei D eine Klausel und für alle Literale $t_1 \neq t_2$ in D gelte $\mathcal{M} \models \mathrm{def}(t_i)$ für $i = 1, 2$. Dann gilt: Aus $\mathcal{M} \models D$ folgt DMod $\models D$.

Bemerkung Sei D eine Klausel.

a) Sei $D \equiv A_1 \wedge \cdots \wedge A_m \Rightarrow B_1 \vee \cdots \vee B_n$ und die A_i, B_j Gleichheitsatome. Der Satz besagt:
Gilt $\mathcal{M} \models \mathrm{def}(t)$ für alle t, die in den A_i auftreten und gilt $\mathcal{M} \models D$, so gilt auch $\mathcal{A} \models D$ für alle Datenmodelle $\mathcal{A}$.

b) Wir entwickeln Hilfsmittel zum Nachweis von DMod(spec) $\models D$.

Konfluenzkriterien (1)

Frage

Wie zeigt man, dass spec $= (\text{sig}, C, R)$ zulässig ist.

Also: Wie zeigt man die Konfluenz von R?

Beachte

Der Konfluenz-Nachweis für R ist i. Allg. schwer, besonders dann, wenn R nicht terminierend ist. Wir formulieren hinreichende Bedingungen mit „kritischen Paaren".

Definition 4.11

Sei $R = R^C \cup R^D$ wie stets.

Seien $\varrho_i \equiv l_i \to r_i \Leftarrow \Delta_i$, $i = 1, 2$, variablen-disjunkte Regeln aus R, sei $\pi \in \text{Pos}(l_2)$ mit $l_2/\pi \notin V$ und sei $\sigma = \text{mgu}(l_1, l_2/\pi)$. Ist $\sigma(l_2[r_1]_\pi) \not\equiv \sigma(r_2)$, so ist

$$\langle(\sigma(l_2[r_1]_\pi), \sigma(\Delta_1), a_1), (\sigma(r_2), \sigma(\Delta_2), a_2)\rangle$$

ein **kritisches Paar** vom Typ (a_1, a_2). Dabei gilt $a_i = 0$, falls $\varrho_i \in R^C$, und $a_i = 1$, falls $\varrho_i \in R^D$.

Das kritische Paar heißt **komplementär**, falls (i) oder (ii) gilt:

i) es gibt ein Atom $u = v$, das in einem $\sigma(\Delta_i)$ positiv und in dem anderen negativ vorkommt.

ii) es gibt t und irreduzible Grundterme u und v, so dass $t = u$ in $\sigma(\Delta_1)$ und $t = v$ in $\sigma(\Delta_2)$ vorkommt.

Konfluenzkriterien (2)

Beispiel

Seien true und false irreduzibel.

Jedes kritische Paar zu $l_1 \to r_1 \Leftarrow \Delta_1$ und $l_2 \to r_2 \Leftarrow \Delta_2$ ist komplementär, falls Δ_1 die Gleichung $u =$ true und Δ_2 entweder $u =$ false oder $u \neq$ true enthält.

Also: Fallunterscheidungen führen häufig zu kritischen Paaren, die komplementär sind.

Definition 4.12

R heißt **links-linear**, falls für jede Regel $l \to r \Leftarrow \Delta$ gilt, dass l keine Variable mehrfach enthält.

R heißt **schwach normal**, falls für jede Regel $l \to r \Leftarrow \Delta$ gilt:

Für jedes $t_1 = t_2$ in Δ gilt für ein $i \in \{1, 2\}$: t_i ist ein irreduzibler Grundterm oder $t_i \in \text{Term}(C, V^C)$ oder es ist $\text{def}(t_i)$ in Δ.

Definition 4.13

R heißt **orthogonal**, falls R linkslinear ist und keine kritischen Paare existieren.

Konfluenzkriterien (3)

Satz 4.2.

Jedes orthogonale R ist konfluent.

ohne Beweis.

Satz 4.3.

Sei spec $= (\text{sig}, C, R)$ eine Spezifikation über spec$^C = (\text{sig}^C, R^C)$.

Sei $R = R^C \cup R^D$ linkslinear und schwach normal.

Sei R^C konfluent und jedes kritische Paar vom Typ $(0, 1)$, $(1, 0)$ oder $(1, 1)$ sei komplementär.

Dann ist R konfluent.

ohne Beweis.

Beachte

Hier wird nicht verlangt, dass R terminierend ist.

Ist R verkleinernd (decreasing), so gibt es schwächere Kriterien an die kritischen Paare, die hinreichend sind für die Konfluenz.

Induktive Gültigkeit

Ziel

Sinnvolle Definition von „Die Klausel D ist gültig in spec“.

2 Ansätze sind naheliegend

a) D gilt in allen Datenmodellen.

b) D gilt in $\mathcal{M}(\text{spec})$.

Wunsch: Monotonie-Eigenschaft

Gilt D in spec und ist spec$'$ eine „vernünftige“ Erweiterung von spec, so gilt D auch in spec$'$. Dies führt zu Ansatz a).

Dann

Man kann beim Aufbau der Spezifikation schritthaltend beweisen. Dabei bleiben bewiesene Aussagen gültig.

Definition 4.14

Sei spec eine zulässige Spezifikation und D eine Klausel. D heißt **gültig** oder ein **induktives Theorem** in spec, falls DMod(spec) $\models D$ gilt.

Konstruktorkonsistente Erweiterungen

Definition 4.15

Seien $\text{spec}_i = (\text{sig}_i, C_i, R_i)$ Spezifikation über $\text{sig}_i = (S_i, F_i, \alpha_i)$ und Variablensystemen V_i für $i = 0, 1$.

spec_1 ist eine **konstruktorkonsistente Erweiterung** von spec_0, falls gilt

(1) $S_0 \subseteq S_1$, $F_0 \subseteq F_1$, $C_0 \subseteq C_1$, $\alpha_0 \subseteq \alpha_1$.

(2) $V_{0,s} = V_{1,s}$ für alle $s \in S_0$.

(3) $R_0 \subseteq R_1$.

(4) Ist $c \in C_1 - C_0$ und $c : s_1 \ldots s_n \to s$, so ist $s \notin S_0$.

(5) Ist $l \to r \Leftarrow u = v$ in $R_1^C - R_0^C$, so ist $l \notin \text{Term}(C_0, V_0)$.

Satz 4.4.

Sei spec_1 eine konstruktorkonsistente Erweiterung von spec_0 und seien $\text{spec}_1, \text{spec}_0$ zulässig. Sei D eine Klausel. Gilt $\text{DMod}(\text{spec}_0) \models D$, so gilt auch $\text{DMod}(\text{spec}_1) \models D$.

ohne Beweis.

Beispiel 1

Sei $F = \{0, s, +, -\}$, $C = \{0, s\}$.

$$R: \begin{array}{l} x + 0 \to x \\ x + s(y) \to s(x + y) \\ x - 0 \to x \\ s(x) - s(y) \to x - y \end{array} \qquad R': \begin{array}{l} x + 0 \to x \\ x + s(y) \to s(x + y) \\ x - 0 \to x \\ s(x) - s(y) \to x - y \\ 0 - y \to 0 \end{array}$$

Sei $\mathcal{M} = \mathcal{M}(\text{spec})$ und $\mathcal{M}' = \mathcal{M}(\text{spec}')$.

$D_1 \equiv (x + y) - y = x$

$D_2 \equiv 0 - s(0) \neq 0$.

Es gilt $\text{DMod}(\text{spec}) \models D_1$, also ist D_1 gültig in spec.

Es gilt $\mathcal{M} \models D_2$, aber $\mathcal{M}' \not\models D_2$. Da $\mathcal{M}'$ ein Datenmodell zu spec ist, gilt nicht $\text{DMod}(\text{spec}) \models D_2$.

Beachte

spec$'$ ist eine konstruktorkonsistente Erweiterung von spec. Definierte man „gültig in spec“ als „gültig in $\mathcal{M}$(spec)“, so bliebe die Gültigkeit nicht erhalten bei konstruktorkonsistenten Erweiterungen.

Beispiel 2

Sei spec wie in Beispiel 1.

Es gilt

DMod(spec) $\models x - y = 0 \wedge y - x = 0 \Rightarrow x = y$.

Beweis:

Sei $\mathcal{A} \in$ DMod(spec), $\sigma : \{x, y\} \to$ Term(C).

Zu zeigen ist
$\mathcal{A} \models \sigma(x) - \sigma(y) = 0 \wedge \sigma(y) - \sigma(x) = 0 \Rightarrow \sigma(x) = \sigma(y)$.
Sei $\sigma(x) = s^i(0)$ und $\sigma(y) = s^j(0)$ und $i \geq j$.

Es gilt $\mathcal{M}$(spec) $\models s^i(0) - s^j(0) = s^{i-j}(0)$, also auch $\mathcal{A} \models s^i(0) - s^j(0) = s^{i-j}(0)$.

Wegen $\mathcal{A} \in$ DMod(spec) gilt $\mathcal{A} \models s^{i-j}(0) = 0 \text{ gdw } i = j$.

Für $i \leq j$ verläuft der Beweis analog mit $\sigma(y) - \sigma(x) = 0$.

Also: Aus $\mathcal{A} \models \sigma(x) - \sigma(y) = 0 \wedge \sigma(y) - \sigma(x) = 0$ folgt $\sigma(x) = \sigma(y)$.

Also
$\mathcal{A} \models \sigma(x) - \sigma(y) = 0 \wedge \sigma(y) - \sigma(x) = 0 \Rightarrow \sigma(x) = \sigma(y)$.

Also DMod(spec) $\models x - y = 0 \wedge y - x = 0 \Rightarrow x = y$.

Beispiel 3

Sei $F = \{0, s, \leq, \text{true}, \text{false}\}$, $C = \{0, s, \text{true}, \text{false}\}$,
$S = \{\text{NAT}, \text{BOOL}\}$,
$R : 0 \leq y \to \text{true}$
$s(x) \leq s(y) \to x \leq y$

Es gilt nicht

DMod(spec) $\models x \leq y = \text{true} \wedge y \leq x = \text{true} \Rightarrow x = y$.

Beweis: Sei $\mathcal{A} = (\mathbb{N}, \mathbb{B}; F^{\mathcal{A}})$, $\mathbb{B} = \{T, F\}$ mit $0^{\mathcal{A}} = 0$, $s^{\mathcal{A}}(x) = x + 1$, $\text{true}^{\mathcal{A}} = T$, $\text{false}^{\mathcal{A}} = F$ und $x \leq^{\mathcal{A}} y = T$ für alle $x, y \in \mathbb{N}$

Dann gilt
$\mathcal{A} \in$ DMod(spec) und
$\mathcal{A} \not\models x \leq y = \text{true} \wedge y \leq x = \text{true} \Rightarrow x = y$,
also nicht DMod(spec) $\models x \leq y = \text{true} \wedge y \leq x = \text{true} \Rightarrow x = y$.

Beachte die Ähnlichkeit zu Beispiel 2.

Es gilt

$\mathcal{M}$(spec) $\models x \leq y = \text{true} \wedge y \leq x = \text{true} \Rightarrow x = y$.

4.3 Der Ansatz von QUODLIBET

Bemerkung

QUODLIBET ist ein in der AG entwickeltes Beweissystem zum Nachweis von induktiven Theoremen zu positiv/negativ bedingten Spezifikationen (mit nur partiell spezifizierten Funktionen).

QUODLIBET

- basiert auf einem Inferenzsystem,
- fasst mehrere Inferenzschritte zu Taktiken zusammen,
- erlaubt die Definition neuer Taktiken,
- ist im Moment nur hochgradig interaktiv einsetzbar.

QUODLIBET

- analysiert die Definitionen der $f \in F - C$,
- arbeitet nur mit freien Konstruktoren,
- erlaubt die Verwendung von Lemmata,
- schlägt sinnvolle Induktionsschemata vor,
- baut Beweisbäume auf,
- erlaubt die Manipulation von Beweisbäumen z. B. durch Aufruf von Taktiken, Ausführung von einzelnen Inferenzschritten, Rücksetzungen von Inferenzfolgen,...

Der prinzipielle Ansatz

QUODLIBET

- arbeitet auf Klauseln,
- verfolgt das Prinzip der Verkleinerung von Gegenbeispielen bis
  a) die Existenz eines Gegenbeispiels evident wird (dann war das Beweisziel kein Theorem) oder
  b) die Nicht-Existenz eines Gegenbeispiels evident wird (dann war das Beweisziel ein Theorem).

Regeln werden auf Klauseln angewandt und sind

- nicht-applikativ
  (z. B. Reinigen einer Klausel oder Aufspaltung nach Fällen) oder
- applikativ
  (z. B. Anwenden einer definierenden Gleichung, eines Lemmas oder einer Induktionsvoraussetzung auf die Klausel).

Verwendung einer Induktionsordnung

- sehr flexibel,
- wird erst spät „geeignet“ festgelegt,
- Nachweis von „kleiner“ zur Anwendung einer Induktionsvoraussetzung ist eine Beweisaufgabe.