Voraussetzungen/Bezeichnungen

Voraussetzungen generell ab jetzt

spec $=$ (sig, E) ist eine (zulässige) Spezifikation.

Die Konstruktoren sind frei, also $E^C = \varnothing$.

Es gibt keine generellen Variablen, also $V^G = \varnothing$ (der Einfachheit halber).

Bezeichnungen (gemäß U. Kühler, Dissertation, 2000)

λ bezeichnet ein Literal.

Γ bezeichnet eine Klausel.

$\langle \Gamma; \omega \rangle$ ist eine **gewichtete Klausel**. (Das Gewicht ω bestimmt die Größe der Klausel.)

(Γ, σ) ist ein **Gegenbeispiel** in $\mathcal{A} \in$ DMod(spec), falls $\mathcal{A} \not\models \sigma(\Gamma)$. Dabei ist σ eine induktive Substitution $\sigma : V^C \to \mathrm{Term}(C)$.

(Γ, σ) ist ein **Gegenbeispiel in spec**, falls $\mathcal{A} \not\models \sigma(\Gamma)$ für ein $\mathcal{A} \in$ DMod(spec).

Lemma 4.6

Sei $\mathcal{A} \in$ DMod(spec). Es gilt $\mathcal{A} \models \Gamma$ gdw es gibt kein Gegenbeispiel (Γ, σ) in $\mathcal{A}$.

DMod(spec) $\models \Gamma$ gdw es gibt kein Gegenbeispiel (Γ, σ) in spec.

Form der Inferenzregeln

Bezeichnung

Ein **Lemma** ist eine Klausel Δ mit DMod(spec) $\models \Delta$. Es ist z. B. jede definierende Gleichung aus E ein Lemma.

Definition 4.16

Eine Inferenzregel hat die Form

$$\frac{\langle \Gamma; \omega \rangle}{\langle \Gamma_1; \omega_1 \rangle, \ldots, \langle \Gamma_n; \omega_n \rangle} \quad \begin{array}{l} \text{mit } \langle \Pi_1; \hat{\omega}_1 \rangle^{U_1}, \ldots, \langle \Pi_k; \hat{\omega}_k \rangle^{U_k} \\ \text{falls Anwendungsbedingung} \end{array}$$

Intention

Die Inferenzregel wird (applikativ) mit den $\langle \Pi_j; \hat{\omega}_j \rangle$ auf das Teilziel $\langle \Gamma; \omega \rangle$ angewandt und erzeugt die neuen Teilziele $\langle \Gamma_i; \omega_i \rangle$. Dabei ist Π_j ein Lemma (dann ist $U_j = \mathcal{L}$) oder ein anderes Teilziel, das als Induktionsvoraussetzung angewendet wird (dann ist $U_j = \mathcal{I}$). Ist $k > 0$, so ist die Regel applikativ. Ist $k = 0$, so ist sie nicht applikativ.

Beachte

Im Fall $n = 0$ wird kein neues Teilziel erzeugt. Wird eine Inferenzregel auf $\langle \Gamma; \omega \rangle$ angewandt, so ist $\langle \Gamma; \omega \rangle$ bearbeitet. Es müssen dann alle neuen Teilziele bearbeitet werden.

Eine Ordnung auf Gegenbeispielen (Motivation)

Definition 4.17

Sei $\mathcal{A} \in$ DMod(spec). Sei Γ eine Klausel und σ eine induktive Substitution. Ein $\mathcal{A}$-**Gegenbeispiel** ist (Γ, σ) mit $\mathcal{A} \not\models \sigma(\Gamma)$, d. h., $\sigma(\Gamma)$ gilt in $\mathcal{A}$ nicht.

Bemerkung

Wir definieren später eine Noethersche Ordnung $\succeq_{\mathcal{A}}$ auf potentiellen $\mathcal{A}$-Gegenbeispielen. Diese wird bezüglich gewichteter Klauseln $\langle \Gamma; \omega \rangle$ definiert, weil das Gewicht ω im wesentlichen die Größe des Gegenbeispiels definiert.

Sei also

$\preceq_{\mathcal{A}}$ eine Ordnung auf den $(\langle \Gamma; \omega \rangle, \sigma)$.

Korrekte Inferenzregeln

Beachte

Die Inferenzregeln sollen Gegenbeispiele verkleinern. Dies spiegelt sich in folgender Definition wider.

Definition 4.18

Eine Inferenzregel

$$\frac{\langle \Gamma; \omega \rangle}{\langle \Gamma_1; \omega_1 \rangle, \ldots, \langle \Gamma_n; \omega_n \rangle} \quad \begin{array}{l} \text{mit } \langle \Pi_1; \hat{\omega}_1 \rangle^{U_1}, \ldots, \langle \Pi_k; \hat{\omega}_k \rangle^{U_k} \\ \text{falls Anwendungsbedingung} \end{array}$$

heißt **korrekt**, falls für jedes $\mathcal{A} \in$ DMod(spec) und jedes $\mathcal{A}$-Gegenbeispiel der Form (Γ, σ) (1), (2) oder (3) gilt.

(1) Es gibt ein $1 \leq i \leq n$ und ein $\mathcal{A}$-Gegenbeispiel der Form (Γ_i, τ), so dass $(\langle \Gamma_i; \omega_i \rangle, \tau) \preceq_{\mathcal{A}} (\langle \Gamma; \omega \rangle, \sigma)$.

(2) Es gibt ein $1 \leq j \leq k$, so dass $U_j = \mathcal{L}$ und Π_j nicht gültig in spec ist.

(3) Es gibt ein $1 \leq j \leq k$ und ein $\mathcal{A}$-Gegenbeispiel der Form (Π_j, τ), so dass $U_j = \mathcal{I}$ und $(\langle \Pi_j; \hat{\omega}_j \rangle, \tau) \prec_{\mathcal{A}} (\langle \Gamma; \omega \rangle, \sigma)$.

Flexible Induktionsordnungen

Bemerkung

Eine Induktionsordnung muss für das Beispiel geeignet sein. Einzige Voraussetzung ist, dass sie Noethersch ist. Also: Wie findet man geeignete Induktionsordnungen?

Die LPO und die RPO sind zwar starke Ordnungen, sie reichen aber häufig nicht aus, da sie rein syntaktisch definiert sind.

Ziel: Semantische Ordnungen benutzen.

Beispiel Quicksort

E : $\text{qsort}(\text{nil}) = \text{nil}$
$\text{qsort}(x.l) = \text{app}(\text{qsort}(\text{lower}(x,l)), x.\text{qsort}(\text{upper}(x,l)))$

Ziel: $\text{sorted}(\text{qsort}(l)) = \text{true}$.

Ein Induktionsbeweis verlangt eine Induktionsordnung, in der $\text{qsort}(x.l)$ größer als $\text{qsort}(\text{lower}(x,l))$ und $\text{qsort}(\text{upper}(x,l))$ ist.

Idee: Wähle $|l|_{\text{sem}} =$ Länge der Liste l.
Zeige $|x.l|_{\text{sem}} > |\text{lower}(x,l)|_{\text{sem}}$.
$|x.l|_{\text{sem}} > |\text{upper}(x,l)|_{\text{sem}}$.

Semantische Ordnung auf $\mathcal{A}$

Sei $\mathcal{A} \in \text{DMod}(\text{spec})$.

Beachte

Da spec zulässig ist und die Konstruktoren frei sind, gibt es zu jedem $a \in A^C$ genau ein $t_a \in \text{Term}(C)$ mit $a = t_a^{\mathcal{A}}$.

Sei $|t_a|$ die Länge von t_a.

Ist $t \in \text{Term}(F)$ und gilt $\mathcal{A} \models \text{def}(t)$, (d. h., t ist in $\mathcal{A}$ definiert), so gibt es genau ein $t_a \in \text{Term}(C)$ mit $t^{\mathcal{A}} = t_a^{\mathcal{A}}$.

Definition 4.19

Die **semantische $\mathcal{A}$-Länge** von $t \in \text{Term}(F)$ ist

$$|t|_{\text{sem}} = \begin{cases} |t_a| & \text{falls } t^{\mathcal{A}} = t_a^{\mathcal{A}}, t_a \in \text{Term}(C) \\ \text{nicht definiert} & \text{sonst} \end{cases}$$

Die **semantische Ordnung** $\succeq_{\mathcal{A}}$ (bzw. $\succ_{\mathcal{A}}$) auf $\text{Term}(F,V)$ ist gegeben durch

$t_1 \succeq_{\mathcal{A}} t_2$ (bzw. $t_1 \succ_{\mathcal{A}} t_2$) gdw $|\sigma(t_1)|_{\text{sem}} \geq |\sigma(t_2)|_{\text{sem}}$ (bzw. $|\sigma(t_1)|_{\text{sem}} > |\sigma(t_2)|_{\text{sem}}$) und $\mathcal{A} \models \text{def}(\sigma(t_i))$ für $i = 1, 2$ und für alle induktiven Substitutionen σ.

Lemma 4.7

$\succ_{\mathcal{A}}$ ist eine Noethersche Partialordnung auf $\text{Term}(F,V)$.

Gilt $t_1 \succeq_{\mathcal{A}} t_2$, so gilt auch $\sigma(t_1) \succeq_{\mathcal{A}} \sigma(t_2)$ für jede Konstruktorsubsitution σ. Analoges gilt für $\succ_{\mathcal{A}}$ statt $\succeq_{\mathcal{A}}$.

Beispiel zur semantischen $\mathcal{A}$-Länge

Sei $F = \{0, s, \mathsf{nil}, ., \mathsf{app}\}$, $C = \{0, s, \mathsf{nil}, .\}$

E : $\mathsf{app}(\mathsf{nil}, l_2) = l_2$
$\mathsf{app}(x.l_1, l_2) = x.\mathsf{app}(l_1, l_2)$

Für $t \in \mathsf{Term}(C)$ gilt $|t|_{\mathsf{sem}} = |t|$,
z. B. $|s^i(0)|_{\mathsf{sem}} = i + 1$
$|s^i(0).s^j(0).\mathsf{nil}|_{\mathsf{sem}} = (i + 1) + (j + 1) + 3$

Für $l_1, l_2 \in \mathsf{Term}(C)$ gilt

$$|\mathsf{app}(l_1, l_2)|_{\mathsf{sem}} = |l_1|_{\mathsf{sem}} + |l_2|_{\mathsf{sem}} - 1.$$

Für jede induktive Subsitution σ und alle $t_1, t_2 \in \mathsf{Term}(F, V)$ gilt

$$|\sigma(\mathsf{app}(t_1, t_2))|_{\mathsf{sem}} = |\sigma(t_1)|_{\mathsf{sem}} + |\sigma(t_2)|_{\mathsf{sem}} - 1.$$

Für alle σ gilt $|\sigma(x.l)|_{\mathsf{sem}} > |\sigma(l)|_{\mathsf{sem}}$ also
$x.l \succ_{\mathcal{A}} l.$

Analog gilt

$$\mathsf{app}(l_1, l_2) \succeq_{\mathcal{A}} l_i \text{ für } i = 1, 2.$$

Beachte

Ist t ein Konstruktorterm und $t >_{TT} s$, so gilt $t \succ_{\mathcal{A}} s$.

Eine Ordnung auf den $(\langle \Gamma; \omega\rangle, \sigma)$

Sei $\mathcal{A} \in \mathsf{DMod}(\mathsf{spec})$ wie stets.

Definition 4.20

Sei $k_0 \in \mathbb{N}$ fest vorgegeben.

Ein **Gewicht** $\omega = (t_1, \ldots, t_k)$ ist ein k-Tupel $\omega \in \mathsf{Term}(F, V)^k$ mit $k \leq k_0$ und $\mathsf{DMod}(\mathsf{spec}) \models \mathrm{def}(t_i)$.

Sei $\succ_{\mathcal{A}}^*$ eine Erweiterung von $\succ_{\mathcal{A}}$ auf die Gewichte $\omega \in \mathsf{Term}(F, V)^k$ etwa die Multimengen-Erweiterung $\succ\!\!\succ_{\mathcal{A}}$ oder die lexikographische Erweiterung $\succ_{\mathcal{A}}^{\mathsf{lex}}$.

Eine Ordnung auf den Gewichten ist von der Form $\succ_{G,\mathcal{A}} = \succ_{\mathcal{A}}^*$.

Eine **Ordnung auf den** $(\langle \Gamma; \omega\rangle, \sigma)$ ist von der Form

$$(\langle \Gamma_1; \omega_1\rangle, \sigma_1) \succeq_{\mathcal{A}} (\langle \Gamma_2; \omega_2\rangle, \sigma_2) \text{ gdw } \sigma_1(\omega_1) \succeq_{G,\mathcal{A}} \sigma_2(\omega_2)$$

Lemma 4.8

$\succeq_{\mathcal{A}}$ ist eine Noethersche Partialordnung auf den $(\langle \Gamma; \omega\rangle, \sigma)$.

Beachte

Damit ist $\succeq_{\mathcal{A}}$ auch eine Noethersche Partialordnung auf den $\mathcal{A}$-Gegenbeispielen $(\langle \Gamma; \omega\rangle, \sigma)$.

Beispiel für einen Induktionsbeweis

Sei $F = \{0, s, \text{true}, \text{false}, \leq\}$, $C = \{0, s, \text{true}, \text{false}\}$.

$E : 0 \leq y = \text{true} \qquad s(x) \leq 0 = \text{false}$
$\quad s(x) \leq s(y) = x \leq y$

$\Gamma : x \leq x = \text{true}$

Struktur eines Beweises

Das 1. Teilziel ist

(1) $\langle x \leq x = \text{true}; x\rangle$

Das Induktionsschema liefert aus (1)

(2) $\langle 0 \leq 0 = \text{true}; 0\rangle$

(3) $\langle s(x) \leq s(x) = \text{true}; s(x)\rangle$

Abarbeitung von (2) mit der Regel Subsumption und $\langle \Pi; \omega\rangle^{\mathcal{L}} = \langle 0 \leq y = \text{true}; y\rangle^{\mathcal{L}}$ liefert kein neues Teilziel.

Abarbeitung von (3) mit der Regel Rewriting und $\langle \Pi; \omega\rangle^{\mathcal{L}} = \langle s(x) \leq s(y) = x \leq y; x\rangle^{\mathcal{L}}$ liefert (4).

(4) $\langle x \leq x = \text{true}; s(x)\rangle$

Abarbeitung von (4) mit der Regel Subsumption und $\langle \Pi; \omega\rangle^{\mathcal{I}} = (1)^{\mathcal{I}}$ liefert kein neues Teilziel. Beachte hierzu $s(x) \succ_{\mathcal{A}} x$, also darf (1) als Induktionsvoraussetzung angewendet werden.

Damit ist der Beweis erfolgreich abgeschlossen: Alle Teilziele sind abgearbeitet.

Ordnungsliterale

Bemerkung

Im letzten Beispiel war die Voraussetzung $s(x) \succ_{\mathcal{A}} x$ für die Anwendbarkeit der Klausel $\langle x \leq x = \text{true}; x\rangle$ auf $\langle x \leq x = \text{true}; s(x)\rangle$ offensichtlich erfüllt. Dies ist i. Allg. nicht der Fall. Im Beispiel qsort benötigt man die Voraussetzungen $x.l \succ_{\mathcal{A}} \text{upper}(x, l)$ und $x.l \succ_{\mathcal{A}} \text{lower}(x, l)$. Dies wird als Beweisaufgabe aufgefasst.

Also: Man benötigt Ordnungsliterale.

Definition 4.21

Ein **Ordnungsatom** hat die Form $\omega_1 < \omega_2$, wobei die ω_i Gewichte sind.

$\mathcal{A} \in \text{DMod(spec)}$ erfüllt $\omega_1 < \omega_2$, falls für jede induktive Subsitution σ gilt $\sigma(\omega_1) \prec_{G,\mathcal{A}} \sigma(\omega_2)$.

Also

Es gibt Gleichheits-, def- und Ordnungsliterale. Das Symbol $<$ wird in $\mathcal{A}$ als kleiner bezüglich der $\mathcal{A}$-Länge interpretiert.

Bemerkung zur Induktionsordnung (1)

Bemerkung

Wir verwenden als Induktionsordnung die Ordnung $\succeq_{\mathcal{A}}$ auf den $(\langle \Gamma; \omega \rangle, \sigma)$. Sie hängt laut Definition von $\mathcal{A}$ ab. Es soll aber die Gültigkeit einer Klausel in allen $\mathcal{A} \in \mathsf{DMod}(\mathsf{spec})$ gezeigt werden.

Also: Wie kann man über alle $\mathcal{A} \in \mathsf{DMod}(\mathsf{spec})$ gleichzeitig schließen?

Beachte

spec ist eine zulässige Spezifikation über freien Konstruktoren. Daraus folgt:

a) Gilt $\mathcal{A}, \mathcal{B} \in \mathsf{DMod}(\mathsf{spec})$, so sind die C-Redukte $\mathcal{A}^C$ und $\mathcal{B}^C$ vermöge $\varphi(t^{\mathcal{A}}) = t^{\mathcal{B}}$, $t \in \mathsf{Term}(C)$, isomorph. Also gilt $|t|^{\mathcal{A}}_{\mathsf{sem}} = |t|^{\mathcal{B}}_{\mathsf{sem}}$ für alle $t \in \mathsf{Term}(C)$.

b) Sei $t \in \mathsf{Term}(F, V)$. Gilt $\mathsf{DMod}(\mathsf{spec}) \models \mathrm{def}(t)$, so gibt es zu jeder induktiven Substitution σ genau ein $t_0 \in \mathsf{Term}(C)$ mit $\mathsf{DMod}(\mathsf{spec}) \models \sigma(t) = t_0$. Also gilt auch hier $|t|^{\mathcal{A}}_{\mathsf{sem}} = |t|^{\mathcal{B}}_{\mathsf{sem}}$.

c) Gilt $\mathsf{DMod}(\mathsf{spec}) \models w_1 < w_2$, so gilt $\mathsf{DMod}(\mathsf{spec}) \models \mathrm{def}(t)$ für alle t, die in w_1 bzw. w_2 vorkommen.

Bemerkung zur Induktionsordnung (2)

Lemma 4.9

Sei $\omega_1 < \omega_2$ ein Ordnungsatom. Gilt $\mathsf{DMod}(\mathsf{spec}) \models \omega_1 < \omega_2$, so gilt $(\langle \Gamma_1; \omega_1 \rangle, \sigma) \prec_{\mathcal{A}} (\langle \Gamma_2; \omega_2 \rangle, \sigma)$ für alle $\mathcal{A} \in \mathsf{DMod}(\mathsf{spec})$.

Beweis: Dies folgt aus dem letzten Beachte.

Also

Da die Gewichte nur aus definierten Termen aufgebaut sind, ist die Induktionsordnung $\succeq_{\mathcal{A}}$ auf den $(\langle \Gamma; \omega \rangle, \sigma)$ für alle $\mathcal{A}$ gleich. Dies erlaubt die Beweisführung für alle $\mathcal{A} \in \mathsf{DMod}(\mathsf{spec})$ gleichzeitig.

Beachte

Der Nachweis der Gültigkeit von $\omega_1 < \omega_2$ in $\mathsf{DMod}(\mathsf{spec})$ kann eine komplizierte Beweisaufgabe sein.

Aber: Gilt $\omega_1 \equiv t_1, \omega_2 \equiv t_2$ und $t_1 <_{TT} t_2$ und $t_1, t_2 \in \mathsf{Term}(C)$, so ist $\omega_1 < \omega_2$ trivialerweise gültig.

Sichere Inferenzregeln: Motivation

Bemerkung

Anschaulich heißt eine Inferenzregel sicher, wenn sie keine neue Gegenbeispiele einführt.

Es ist manchmal durchaus sinnvoll, unsichere Regeln zu betrachten, z. B. die Generalisierung:

Spezifiziert seien die natürlichen Zahlen mit $+$ und $\cdot$ als definierte Operatoren. Zu zeigen sei $x \cdot x + y \cdot y = y \cdot y + x \cdot x$. Dies kann man generalisieren zur Behauptung $x + y = y + x$. Aus ihr folgt die eigentliche Behauptung, sie ist aber viel leichter zu zeigen.

Für die Lemma-Spekulation und -Verarbeitung gibt es in QUODLIBET einen eigenen Mechanismus.

Sichere Inferenzregeln: Definition

Definition 4.22

$$\frac{\langle \Gamma; \omega \rangle}{\langle \Gamma_1; \omega_1 \rangle, \ldots, \langle \Gamma_n; \omega_n \rangle} \quad \begin{array}{l} \text{mit } \langle \Pi_1; \hat{\omega}_1 \rangle^{U_1}, \ldots, \langle \Pi_k; \hat{\omega}_k \rangle^{U_k} \\ \text{falls Anwendungsbedingung} \end{array}$$

heißt **sicher**, falls gilt: Sind Γ und die Π_i gültig in DMod(spec), so ist auch jedes Γ_j gültig in DMod(spec).

Beachte

Ist Γ gültig und $\Gamma \subseteq \Gamma_j$, so ist auch Γ_j gültig.

Lemma 4.10

Gilt $\Gamma \subseteq \Gamma_j$ für alle $j = 1, \ldots, n$, so ist die Inferenzregel sicher.

Bemerkung

Fast alle Inferenzregeln von QUODLIBET sind sicher aufgrund dieses Lemmas.

Ist $\Gamma_j = \Gamma \cup \Lambda_j$, so reicht es zu zeigen, dass ein $\lambda \in \Gamma_j$ gültig ist. Häufig ist es sinnvoll, dazu ein $\lambda \in \Lambda_j$ zu wählen. Die $\lambda' \in \Gamma$ dienen nur zur „Sicherung“, falls kein $\lambda \in \Lambda_j$ gültig ist.

Verallgemeinerte Substitutionen

Erinnerung

Für eine Substitution σ gilt $\sigma(x) \in \text{Term}(C, V^C)$ für alle $x \in V^C$.

Es ist sinnvoll, auch Substitutionen mit $\sigma(x) \in \text{Term}(F, V^C)$ zuzulassen, aber nur dann, wenn $\sigma(x)$ definiert ist, d. h., wenn DMod(spec) $\models \mathrm{def}(\sigma(x))$ gilt.

Definition 4.23

$\sigma : V^C \to \text{Term}(F, V^C)$ heißt **verallgemeinerte Substitution**, falls DMod(spec) $\models \mathrm{def}(\sigma(x))$ für alle $x \in V^C$ gilt.

Also

Benutzt man in einer Regelanwendung eine verallgemeinerte Subsubstitution, so muss man jedes x mit $\sigma(x) \notin \text{Term}(C, V^C)$ durch das Literal $\mathrm{def}(\sigma(x))$ bewachen. Dieses Literal lässt sich leicht beweisen, falls $\sigma(x) \in \text{Term}(C \cup F^d, V^C)$ ist, wobei F^d aus allen total definierten Funktionssymbolen $f \in F$ besteht. QUODLIBET testet für die Spezifikation der $f \in F$, ob f total definiert ist.

4.4 Die Inferenzregeln

Beachte

Ein Ziel hat die Form $\langle \Gamma; \omega \rangle$ mit

$$\Gamma = (\lambda_1, \ldots, \lambda_n) \qquad \omega = (t_1, \ldots, t_m)$$

Also: Γ ist eine Folge von Literalen.

Regeln transformieren Ziele in Teilziele.

Wir benötigen Regeln für
a) das (triviale) Säubern von Klauseln,
b) die Behandlung von $=$ und $\neq$,
c) die Behandlung von def,
d) die Behandlung von Gewichten, also von $<$,
e) das Anwenden von sicherem Wissen, also eines Axioms oder Lemmas,
f) das Anwenden von Induktionsvoraussetzungen,
g) die Durchführung von Fallunterscheidungen.

Bezeichnung

$=_{\text{lit}}$ ist die Gleichheit auf Literalen.

Beispiele

Sei $\lambda_1 \equiv A$, $\lambda_2 \equiv \neg A$, A ein Atom. Es ist $\lambda_1 =_{\text{lit}} \overline{\lambda_2}$.

Sei $\lambda_1 \equiv s = t$, $\lambda_2 \equiv t = s$. Es ist $\lambda_1 =_{\text{lit}} \lambda_2$.