Beispiel 2

$\mathcal{A}x : \forall x, y.[x + 0 = x \wedge x + s(y) = s(x + y) \wedge$
$\quad d(0) = 0 \wedge d(s(x)) = s(s(d(x)))].$

$\varphi : \forall x \exists y.\ d(x) = y + y.$

Dies liefert

$$E : x + 0 = x \qquad x + s(y) = s(x + y)$$
$$d(0) = 0 \qquad d(s(x)) = s^2(d(x)).$$

$Z : d(a) = y + y.$

Sei σ eine beliebige Grundsubstitution. Dann enthält $\sigma(y + y)$ n Vorkommen von a mit $n = 0$ oder $n > 1$. Wegen der speziellen Gestalt der Gleichungen in E enthält auch jeder Term t mit $t =_E \sigma(y + y)$ genau n a's.

Also gilt nicht $\sigma(d(a)) =_E \sigma(y + y)$.

Also gilt nicht $\mathcal{A}x \models \varphi$.

Übung: Man teste, ob gilt

a) $\mathcal{A}x \models \forall x.[x = 0 \vee \exists y.x = s(y)]$.

b) $\mathcal{A}x \models \forall x, y.[d(x) = y \Rightarrow d(d(x)) = d(y))$.

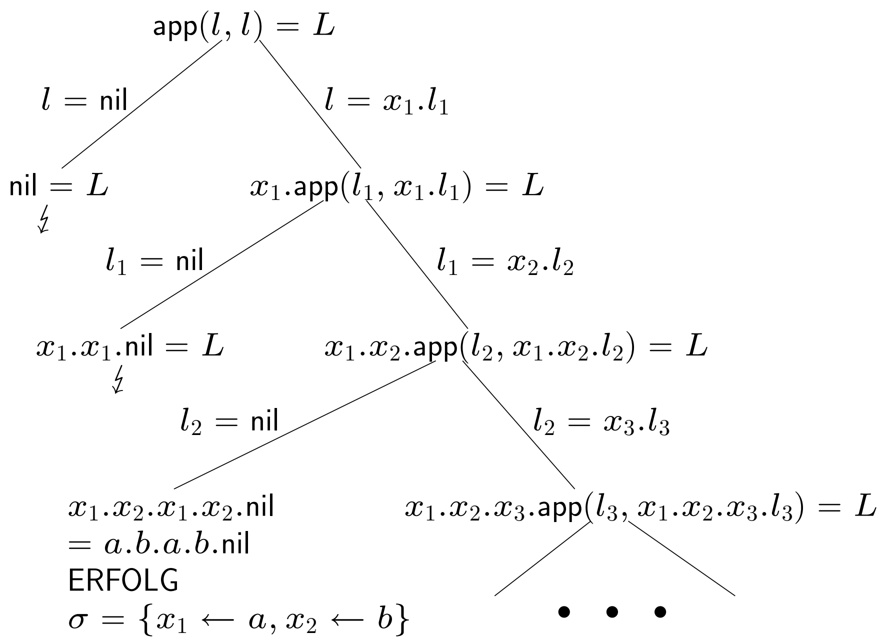
c) $\mathcal{A}x \models \forall x, y.[d(x) = y \Rightarrow d(y) = d(x) + d(x)]$.

Beispiel Narrowing

$R : \quad \mathsf{app}(\mathsf{nil}, l_2) \to l_2$
$\quad \mathsf{app}(x.l_1, l_2) \to x.\mathsf{app}(l_1, l_2)$

Gesucht: R-Lösungen zu $\mathsf{app}(l, l) = a.b.a.b.\mathsf{nil} \equiv L$

Narrowing: Suchbaum



$\rightsquigarrow \sigma(l) = a.b.\mathsf{nil}$ ist eine R-Lösung zu $\mathsf{app}(l, l) = a.b.a.b.\mathsf{nil}$

Beispiel

$$\mathcal{A}x: \quad \begin{array}{l} \forall x. x \cdot 1 = x \\ \forall x. x \cdot x = x \\ \forall x. \forall y. \forall z. (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \qquad \varphi \equiv \exists x. \exists y. x \cdot y = y \cdot x$$

Frage: Gilt $\mathcal{A}x \models \varphi$?

Dies liefert

- $E: x \cdot 1 = x \quad x \cdot x = x \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Ist $x' \cdot y' = y' \cdot x'$ E-lösbar?

Vervollständigung liefert

(1) $1 \cdot x \to x$ Also

$$\begin{tikzcd}
 & x' \cdot y' = y' \cdot x' \arrow[dl, "y' = 1"'] \arrow[dr, "x' = 1"] & \\
x' \cdot 1 = x' \arrow[d] & & y' = y' \cdot 1 \arrow[d] \\
x' = x' & & y' = y'
\end{tikzcd}$$

$\rightsquigarrow \sigma = \{y' \leftarrow 1\}$ $\quad \rightsquigarrow \sigma = \{x' \leftarrow 1\}$

(2) $x \cdot y = y \cdot x$ Also

$$\begin{tikzcd}
x' \cdot y' = y' \cdot x' \arrow[d] \\
x' \cdot y' = x' \cdot y'
\end{tikzcd}$$

$\rightsquigarrow \sigma = \mathrm{id}$

Also gilt sogar $x' \cdot y' =_E y' \cdot x'$

also $\mathcal{A}x \models \forall x. \forall y. x \cdot y = y \cdot x$

4 Theorembeweisen in PL1

Ziel von Kapitel 4

Darstellung des Superpositionskalküls.

Beachte

Die heute schnellsten Beweiser beruhen auf diesem Kalkül.

Problemstellung

Gegeben: S, eine Menge von Klauseln.

Aufgabe: Zeige, dass S Herbrand-unerfüllbar ist.

Bemerkung

Der Superpositionskalkül baut auf folgenden Kalkülen auf

- Resolution,
- Paramodulation.

Wir führen diese Kalküle ein.

Beschreibung von Kalkülen

Wir schreiben Inferenzregeln jetzt etwas anders als in Kapitel 3.

Bezeichnung

Ein **Kalkül** $\mathcal{K}$ wird beschrieben durch ein System von Inferenzregeln, die auf Formelmengen S arbeiten.

Eine **Inferenzregel** hat die Form

$$\frac{C_1, \ldots, C_n}{D} \qquad \text{falls Anwendungsbedingung}$$

mit $n \geq 0$, wobei die C_i, D Formeln sind.

Wir schreiben $S \underset{\mathcal{K}}{\vdash} S'$, falls es solch eine Inferenzregel gibt mit $C_1, \ldots, C_n \in S$ und $S' = S \cup \{D\}$.

Eine $\mathcal{K}$-**Ableitung** ist eine Folge $(S_i)_{i \in \mathbb{N}}$ mit $S_i \underset{\mathcal{K}}{\vdash} S_{i+1}$ für alle $i \geq 0$. Sie kann endlich oder unendlich sein.

Wir schreiben $S \overset{*}{\underset{\mathcal{K}}{\vdash}} C$, falls es eine $\mathcal{K}$-Ableitung $(S_i)_{i \in \mathbb{N}}$ gibt mit $S = S_0$ und $C \in S_k$ für ein $k \geq 0$.

Hier

Die Formeln sind Klauseln, also ist S eine Klauselmenge.

Bemerkungen

Bemerkung

Wir schreiben $\mathcal{K}$-Ableitungen auch als Folge von Formeln. Eine $\mathcal{K}$-**Herleitung** aus S ist eine Folge $C'_1, \ldots, C'_m$, so dass für alle $1 \leq i \leq m$ gilt

a) $C'_i \in S$ oder

b) es gibt eine Inferenzregel $\dfrac{C_1, \ldots, C_n}{D}$, so dass die C_j unter den $C'_1, \ldots, C'_{i-1}$ vorkommen und $D \equiv C'_i$ ist.

Ist $C \equiv C'_m$, so ist dies eine $\mathcal{K}$-Herleitung von C aus S.

Schreibweise $S \overset{*}{\underset{\mathcal{K}}{\vdash}} C$.

Beachte

Uns interessieren Kalküle zum Nachweis der H-Unerfüllbarkeit von S. Die leere Klausel $\Box$ ist unerfüllbar. Ziel ist es also, $S \overset{*}{\underset{\mathcal{K}}{\vdash}} \Box$ zu zeigen.

Definition 4.1.

$\mathcal{K}$ heißt **korrekt**, falls aus $S \overset{*}{\underset{\mathcal{K}}{\vdash}} \Box$ folgt, dass S H-unerfüllbar ist.

$\mathcal{K}$ heißt **vollständig**, falls gilt: Ist S H-unerfüllbar, so gilt $S \overset{*}{\underset{\mathcal{K}}{\vdash}} \Box$.

Beispiel: Vervollständigungskalkül

Die Inferenzregel „Bildung kritisches Paar“ lautet

$$\frac{l = r \quad u = v}{\sigma(r) = \sigma(l[v]_\pi)} \quad \text{falls } \begin{array}{l} \pi \in \mathrm{Pos}(l), l/\pi \notin V, \\ \sigma = mgu(u, l/\pi), \\ \sigma(l) \not> \sigma(r) \not< \sigma(l[v]_\pi) \end{array}$$

Übung

1. Man beschreibe die KB-Vervollständigung als Kalkül $\mathcal{K}_{KB}$.
2. Sei $S = \{a = b, a = c, b = d\}$ und $>$ die RPO mit $a >_F b >_F c >_F d$. Man gebe eine $\mathcal{K}_{KB}$-Ableitung von $S \vdash c = d$ an.

Zur Korrektheit von $\mathcal{K}$

Definition 4.2.

Eine Inferenzregel $\dfrac{C_1, \ldots, C_n}{D}$ heißt **korrekt**, falls gilt: Ist $\{C_1, \ldots, C_n\}$ H-erfüllbar, so ist es auch $\{C_1, \ldots, C_n, D\}$.

Lemma 4.1

Ist jede Inferenzregel von $\mathcal{K}$ korrekt, so ist auch der Kalkül $\mathcal{K}$ korrekt.

Beweis:

Sei $S \overset{*}{\underset{\mathcal{K}}{\vdash}} \Box$, also $S_0, \ldots, S_n$ eine $\mathcal{K}$-Ableitung mit $S_0 = S$ und $\Box \in S_n$. Ist S_0 H-erfüllbar, so ist jedes S_i H-erfüllbar (Induktion nach i). Wäre S H-erfüllbar, so wäre auch S_n H-erfüllbar, wegen $\Box \in S_n$ also auch $\Box$. Das ist unmöglich.

Also ist S unerfüllbar.

Also ist $\mathcal{K}$ korrekt.

Beachte

Die Korrektheit von $\mathcal{K}$ ist häufig leicht zu zeigen. Schwierig ist der Nachweis der Vollständigkeit.

4.1 Resolution und Paramodulation

Resolution für PL1

Sei $=$ nicht in P, also die Gleichheit ausgeschlossen.
S eine Menge von Klauseln über sig $= (F, P, \alpha)$.
Seien A, B Atome, l_1, l_2 Literale, C, D Klauseln.

Definition 4.3.

Der **Resolutionskalkül** $\mathcal{R}$ besteht aus 2 Inferenzregeln:

Resolution

$$\frac{C \vee A \quad D \vee \neg B}{\sigma(C \vee D)} \qquad \text{falls } \sigma = \mathrm{mgu}(A, B)$$

Faktorisierung

$$\frac{C \vee l_1 \vee l_2}{\sigma(C \vee l_1)} \qquad \text{falls } \sigma = \mathrm{mgu}(l_1, l_2)$$

Ziel

Der Resolutionskalkül ist korrekt und vollständig:

$S \overset{*}{\underset{\mathcal{R}}{\vdash}} \Box \ \text{ gdw } \ S$ ist H-unerfüllbar.

Beispiel zur Resolution

Beispiel: Quacksalber

Sei $S = \{(1), \ldots, (5)\}$, siehe Einleitung.

(1) pat(a)
(2) $\neg$doc$(y) \vee$ mag(a, y)
(3) $\neg$pat$(x') \vee \neg$qua$(y') \vee \neg$mag(x', y')
(4) doc(b)
(5) qua(b)

Anwendung der Resolutionsregel liefert

(6) $\neg$qua$(y'') \vee \neg$mag(a, y'') mit (1), (3)
(7) $\neg$mag(a, b) mit (5), (6)
(8) mag(a, b) mit (2), (4)
(9) $\Box$ mit (7), (8)

Also ist S nicht H-erfüllbar.

Also gilt $\mathcal{A}x \models \forall x.(\mathrm{doc}(x) \Rightarrow \neg\mathrm{qua}(x))$ mit
$\mathcal{A}x = \{\exists x.(\mathrm{pat}(x) \wedge \forall y.(\mathrm{doc}(y) \Rightarrow \mathrm{mag}(x, y))),$
$\quad \forall x.(\mathrm{pat}(x) \Rightarrow \forall y.(\mathrm{qua}(y) \Rightarrow \neg\mathrm{mag}(x, y)))\}$

Literatur-Hinweis

J.A. Robinson: A machine-oriented logic based on the resolution principle, J. ACM 12 (1965) 23-41.

Korrektheit von $\mathcal{R}$

Erinnerung

Ein Herbrand-Modell über der Signatur sig $= (F, P, \alpha)$ ist festgelegt durch die Teilmenge $I \subseteq \{A \mid A \text{ ist Grundatom}\}$. Die Intention ist: $A \equiv p(t_1, \ldots, t_n)$ gilt in dem Modell genau dann, wenn $A \in I$ ist. Also gilt für jede Grundklausel C:

I ist Modell zu C gdw es gibt $A \in C$ mit $A \in I$ oder
$\neg A \in C$ mit $A \notin I$.

Lemma 4.2

Für die Regeln $\dfrac{C_1, \ldots, C_n}{D}$ $(n = 1, 2)$ des Resolutionskalküls gilt: Ist I ein Modell von $\{C_1, \ldots, C_n\}$, so ist I auch ein Modell von $\{C_1, \ldots, C_n, D\}$.

Beweis: Es hat D die Form $D \equiv \sigma(D_0)$. Es reicht für jede Grundsubstitution τ zu zeigen: Ist I ein Modell für alle $\tau(\sigma(C_i))$, so ist I auch ein Modell für $\tau(\sigma(D_0))$.

Übung: Man zeige dies für beide Inferenzregeln von $\mathcal{R}$.

Lemma 4.3

Der Resolutionskalkül $\mathcal{R}$ ist korrekt.

Beweis: Dies folgt aus Lemma 4.1 und 4.2.

Bemerkung zur Vollständigkeit von $\mathcal{R}$

Bemerkung

Der Vollständigkeitsbeweis für $\mathcal{R}$ ist viel schwieriger als der Korrektheitsbeweis.

Wir betrachten erst den Fall, dass S eine Menge von Grundklauseln ist und „liften" das Ergebnis auf den allgemeinen Fall.

Beachte

Für Grundklauseln reduziert sich $\mathcal{R}$ auf die Inferenzregeln

$$\frac{A \vee C \qquad \neg A \vee D}{C \vee D} \qquad \text{Resolution}$$

$$\frac{A \vee A \vee C}{A \vee C} \qquad \text{positive Faktorisierung}$$

$$\frac{\neg A \vee \neg A \vee C}{\neg A \vee C} \qquad \text{negative Faktorisierung}$$