10 Gleichheitsbehandlung

Das bekannte Leibnizsche Prinzip besagt, daß zwei Dinge gleich sind, wenn sie bezüglich aller ihrer Eigenschaften gleich sind. In jedem beliebigen Kontext kann daher "Gleiches durch Gleiches" ersetzt werden. Diese grundlegende Eigenschaft wird so häufig ausgenutzt, daß sie wohl jedem geläufig ist, der schon mit Gleichungen hantiert hat.

Traditionell wird die Gleichheit mit dem binären Symbol "=" bezeichnet.

In einer Logik höherer Ordnung kann man Gleichhheit leicht definieren und erklären durch:

$$\forall x, y : x = y \Leftrightarrow \forall P : P(x) \Leftrightarrow P(y)$$

Allerdings ist das nicht direkt in PL_1 übersetzbar.

Beispiel 10.1. Der Beweis des folgenden Theorems zeigt, welche typischen Schwierigkeiten bei Gleichheitsbeweisen auftreten. Zu zeigen sei: Eine Gruppe mit $\forall x : x^2 = 1$ ist kommutativ. Die Axiome einer Gruppe mit einem zweistelligen Verknüpfungssymbol $\bullet$ und einer einstelligen Funktion i (Inverses) sind:

$$\forall x, y, z : (x \bullet y) \bullet z = x \bullet (y \bullet z) \qquad \text{(Assoziativität)}$$

$$\forall x : \quad 1 \bullet x = x \qquad \text{(Links-Eins)}$$

$$\forall x : \quad x \bullet 1 = x \qquad \text{(Rechts-Eins)}$$

$$\forall x : \quad i(x) \bullet x = 1 \qquad \text{(Links-Inverses)}$$

$$\forall x : \quad x \bullet i(x) = 1 \qquad \text{(Rechts-Inverses)}$$

Als zusätzliche Voraussetzung soll gelten:

$$\forall x \quad x \bullet x = 1 \qquad \text{(Voraussetzung)}$$

Die Behauptung ist nun:

$$\forall x, y : \quad x \bullet y = y \bullet x$$

Ein Beweis der Kommutativität wird zum Beispiel durch folgende Gleichungskette geführt:

$$
\begin{array}{lll}
(1)\ x \bullet y = (1 \bullet x) \bullet y & & \text{(Links-Eins)} \\
(2) & = ((y \bullet y) \bullet x) \bullet y & \text{(Voraussetzung)} \\
(3) & = ((y \bullet y) \bullet x) \bullet (y \bullet 1) & \text{(Rechts-Eins)} \\
(4) & = ((y \bullet y) \bullet x) \bullet (y \bullet (x \bullet x)) & \text{(Voraussetzung)} \\
(5) & = (y \bullet ((y \bullet x) \bullet (y \bullet x))) \bullet x & \text{(mehrmals Assoziativität)} \\
(6) & = (y \bullet 1) \bullet x & \text{(Voraussetzung)} \\
(7) & = y \bullet x & \text{(Rechts-Eins)}
\end{array}
$$

Der Beweistrick besteht darin, an den richtigen Stellen mit dem Einselement zu erweitern, das Einselement durch Anwendung der Voraussetzung geschickt darzustellen, umzuklammern und wieder zusammenzufassen. Welche der Umformungen in jedem einzelnen Schritt durchgeführt werden müssen, um zum Ziel zu kommen, ist zunächst jedoch überhaupt nicht zu erkennen. Zum Beispiel wären nach Schritt (3) auch die Operationen

$$
\begin{array}{ll}
(3)\quad ((y \bullet y) \bullet x) \bullet (y \bullet 1) = (1 \bullet x) \bullet (y \bullet 1) & \text{(Voraussetzung)} \\
\text{oder } ((y \bullet y) \bullet x) \bullet (y \bullet 1) = ((y \bullet y) \bullet x) \bullet (y \bullet (1 \bullet 1)) & \text{(Links- oder Rechts-Eins)} \\
\text{oder } ((y \bullet y) \bullet x) \bullet (y \bullet 1) = ((y \bullet y) \bullet x) \bullet ((y \bullet 1) \bullet 1) & \text{(Rechts-Eins)} \\
\text{oder } ((y \bullet y) \bullet x) \bullet (y \bullet 1) = ((y \bullet y) \bullet x) \bullet ((1 \bullet y) \bullet 1) & \text{(Links-Eins)} \\
\text{oder } ((y \bullet y) \bullet x) \bullet (y \bullet 1) = (y \bullet (y \bullet x)) \bullet (y \bullet 1) & \text{(Assoziativität)} \\
\text{oder } ((y \bullet y) \bullet x) \bullet (y \bullet 1) = ((y \bullet y) \bullet x) \bullet (y \bullet (i(w) \bullet w)) & \text{(Links-Inverses)}
\end{array}
$$

sowie noch etliche andere ausführbar. Von jedem dieser nutzlosen Schritte aus gibt es wiederum eine Vielzahl weiterer alternativer Umformungen, so daß durch reines Ausprobieren aller Möglichkeiten ca. 10^{11} Versuche notwendig sind, um endlich zur anderen Seite der Gleichung zu kommen.

10.1 Formalisierung der Gleichheit innerhalb der Prädikatenlogik

In PL_1 kann das Gleichheitsprädikat $=$ nur dann durch eine endliche Axiomenmenge formalisiert werden, wenn man die Signatur (Funktionssymbole, Prädikatensymbole) kennt und wenn diese endlich ist. Eine unabhänigige Axiomatisierung ist erst in Logik einer höheren Stufe möglich. In PL_1 kann man stattdessen die benötigte Axiomenmenge durch Instantiierung eines "Axiomenschemas" erzeugen:

Definition 10.2. *Axiomenschema für die Gleichheit:*

$$\forall x : \quad x = x \qquad \textit{(Reflexivität)}$$

$$\forall x, y : \quad x = y \Rightarrow y = x \qquad \textit{(Symmetrie)}$$

$$\forall x, y, z : \quad x = y \wedge y = z \Rightarrow x = z \qquad \textit{(Transitivität)}$$

Für jedes Argument von jedem in der Formelmenge vorkommenden

Funktionssymbol f wird ein Substitutionsaxiom folgender Form benötigt:

$$\forall x_1, \ldots, x_n, y : x_i = y \Rightarrow f(x_1, \ldots, x_i, \ldots, x_n) = f(x_1, \ldots, y, \ldots, x_n)$$

Für jedes Argument von jedem in der Formelmenge vorkommenden

Prädikatensymbol P wird ebenfalls ein weiteres Substitutionsaxiom benötigt:

$$\forall x_1, \ldots, x_n, y : x_i = y \wedge P(x_1, \ldots, x_i, \ldots, x_n) \Rightarrow P(x_1, \ldots, y, \ldots, x_n)$$

Eine naive Methode, um Gleichheitsbeweise im Rahmen der Prädikatenlogik zu automatisieren, wäre also, zu den gegebenen Formeln nach dem obigen Schema die nötigen Gleichheitsaxiome hinzuzufügen und dann mit Resolution einen Beweis zu suchen. Wenn man das für das Gruppenbeispiel von oben durchführt und den Beweis im Resolutionskalkül nachrechnet, wird man feststellen, daß erstens die einzelnen Umformungsschritte sehr umständlich durch mehrere Resolutionsschritte nachgebildet werden müssen, und daß zweitens der Suchraum durch neue Ableitungsmöglichkeiten mit den Gleichheitsaxiomen noch weiter anwächst, in diesem Fall bis auf ca. 10^{21} Ableitungen bei reiner Breitensuche. Diese Vorgehensweise ist also nicht praktikabel.

Da die Formalisierung der Gleichheit mit den obigen Axiomen nicht zu brauchbaren Ergebnissen führt, hat man schon früh versucht, diese Relation unmittelbar in die Logik einzubauen. In den jeweiligen Kalkülen können dann spezielle Ableitungsoperationen, die deren Bedeutung direkt ausnutzen, formuliert werden.

Der *modelltheoretische* Einbau in die Logik geschieht, indem man von allen möglichen Interpretationen für Formeln nur noch diejenigen zuläßt, bei denen das Symbol = die Identität in Σ-Strukturen abgebildet wird. Die heißen dann E-Interpretationen (E von equality) oder Gleichheitsinterpretationen. Äquivalent ist, daß die Gleichheit eine Kongruenz auf der Menge der Elemente des Modells ist.

Mit Hilfe der E-Interpretationen lassen sich jetzt die anderen semantischen Begriffe wie E-Modelle, E-Folgerung, E-erfüllbar und E-unerfüllbar in der üblichen Weise definieren.

10.2 Paramodulation

Eine natürliche, in der Mathematik häufig verwendete Regel zur Behandlung der Gleichheit beruht auf dem Prinzip der Untertermersetzung: In beliebigem Kontext kann Gleiches durch Gleiches ersetzt werden. Ähnlich wie bei Resolution ist auch hierbei in vielen Fällen die Anwendung einer Instantiierungsregel nötig, um die Voraussetzungen für die Anwendbarkeit der Untertermersetzung herzustellen, wobei Unifikation willkürliche Instantiierungen überflüssig macht und stattdessen ein zielgerichtetes Instantiieren auf der allgemeinsten Ebene ermöglicht. So wie der Modus Ponens unter Verwendung des Unifikationsprinzips zur Resolution verallgemeinert wurde, haben G. Robinson und L. Wos auch die Gleichheitsersetzungsregel zur Paramodulationsregel verallgemeinert.

Formal wird die Paramodulationsregel wie folgt definiert:

Definition 10.3. (Paramodulation)

$$\begin{array}{ll} C_1 & := \{L_1[s], L_2, \ldots, L_n\} \\ C_2 & := \{l = r, K_2, \ldots, K_m\} \\ \hline P & := \sigma\{L_1[r], L_2, \ldots, L_n, K_2, \ldots, K_m\} \end{array}$$

Hierbei enthält $L_1[s]$ den Unterterm s, s und l sind unifizierbar mit dem allgemeinsten Unifikator σ (d.h. $\sigma s \equiv \sigma l$) und P ist Paramodulant *der Klauseln C_1 und C_2, wobei $L_1[r/s]$ aus L_1 durch Ersetzen des Terms s durch den Term r entsteht.*

Paramodulation könnte man als bedingte Ersetzung bezeichnen, wobei die restlichen Literale der Klauseln wie Bedingungen wirken und in der Paramodulante die Bedingungen aufgesammelt werden. Die einfachste Variante ist die Paramodulation ohne Bedingungen. Dies wird auch *Termersetzung* genannt:

$$\begin{array}{ll} C_1 & := \{L[s]\} \\ C_2 & := \{l = r\} \\ \hline P & := \sigma\{L[r]\} \end{array}$$

wobei σ allgemeinster Unifikator von s und l.

Beispiel 10.4. Für einen Paramodulationsschritt.

$$\begin{aligned} C_1 &:= \{P(c, h(f(a, y), b))\} \\ C_2 &:= \underline{\{f(x, e) = g(x), Q(x)\}} \\ P\ &:= \{P(c, h(g(a), b)), Q(a)\} \end{aligned}$$

$P = \{P(c, h(g(a), b)), Q(a)\}$ ist Paramodulant der beiden Klauseln. Die Terme $f(a, y)$ und $f(x, e)$ sind unifizierbar mit $\{x \mapsto a, y \mapsto e\}$. Diese Substitution muß auf die neue Klausel angewendet werden.

Paramodulation ist in zweifacher Hinsicht allgemeiner als die oben erwähnte Regel "Gleiches durch Gleiches zu ersetzen":

1. Paramodulation ist nicht nur mit unbedingten, sondern auch mit bedingten Gleichungen anwendbar, das heißt die Gleichungs-Klausel kann noch weitere Literale enthalten.
2. Die beiden Terme, welche eine Ersetzung ermöglichen sollen, müssen nicht gleich, sondern lediglich unifizierbar sein, was bedeutet, daß es Instanzen der beteiligten Klauseln geben muß, so daß die entsprechenden Terme gleich sind.

10.3 Eigenschaften der Paramodulation

Die Paramodulationsregel ist korrekt: falls S eine E-erfüllbare (bzw. E-unerfüllbare) Menge von Klauseln und C Paramodulant von zwei Klauseln aus S ist, dann ist auch $S \cup \{C\}$ E-erfüllbar (bzw. E-unerfüllbar).

Erweitert man den Resolutionskalkül um die Paramodulationsregel und erweitert die Eingabeklauseln um die Klausel (das Axiom) $\{x = x\}$, dann erhält man den RP-Kalkül für die Prädikatenlogik erster Stufe mit Gleichheit.

> Dieser ist widerlegungsvollständig: für jede E-unerfüllbare Menge von Klauseln existiert eine Ableitung der leeren Klausel unter Anwendung der Regeln und Axiome des Kalküls.

Das Reflexivitätsaxiom ist nötig, da andernfalls die leere Klausel nicht aus der E-unerfüllbaren, einelementigen Klauselmenge $\{\{\neg a = a\}\}$ ableitbar wäre.

Verglichen mit der expliziten Verwendung der Gleichheitsaxiome ist der Suchraum für die Ableitung der leeren Klausel durch Einführung der Paramodulation deutlich kleiner. Viele der sinnlosen Resolutionen mit und zwischen den Gleichheitsaxiomen sind nicht mehr möglich. Trotzdem sind die entstehenden Suchräume ohne geschickte heuristische Steuerung der Paramodulation noch viel zu groß, da auch diese Regel fast überall in der Klauselmenge angewendet werden kann. Für das obige Gruppenbeispiel sind nach Alan Bundy bei reiner Breitensuche etwa 10^{11} Paramodulationsschritte versuchsweise nötig, um den Beweis des Satzes zu finden.

Beispiel 10.5. für Kombination von Resolution und Paramodulation.
Zu zeigen ist: Das Einselement einer Untergruppe ist dasselbe wie das Einselement der Gruppe selbst.

Axiomatisierung:

$$\forall X, Y : X \subseteq Y \Rightarrow (\forall x : x \in X \Rightarrow x \in Y) \qquad \text{(Teilmengenbeziehung)}$$

$$\forall X : Gruppe(X) \Rightarrow (\forall x : x \in X \Rightarrow x * inv(x) = id(X)) \qquad \text{(Def. Einselement)}$$

$$\forall X : Gruppe(X) \Rightarrow id(X) \in X$$

$$\forall X, Y : Gruppe(X) \wedge Gruppe(Y) \wedge X \subseteq Y \Rightarrow id(X) = id(Y) \text{ (Theorem)}$$

Klauselform:

$$C1 : \neg X \subseteq Y, \neg x \in X, x \in Y$$

$$C2 : \neg Gruppe(X), \neg x \in X, x * inv(x) = id(X)$$

$$C3 : \neg Gruppe(X), id(X) \in X$$

$$T1.\ \ Gruppe(A)$$

$$T2 : Gruppe(B)$$

$$T3 : A \subseteq B$$

$$T4 : id(A) \neq id(B)$$

Resolutions- und Paramodulationswiderlegung:

$$
\begin{array}{ll}
C1,1+T3 & \vdash R1: \neg x \in A, x \in B \\
C2,1+T1 & \vdash R2: \neg x \in A, x * inv(x) = id(A) \\
C3,1+T1 & \vdash R3: id(A) \in A \\
R2,1+R3 & \vdash R4: id(A) * inv(id(A)) = id(A) \\
C2,1+T2 & \vdash R5: \neg x \in B, x * inv(x) = id(B) \\
R1,2+R5,1 & \vdash R6: \neg x \in A, x * inv(x) = id(B) \\
R6,1+R3 & \vdash R7: id(A) * inv(id(A)) = id(B) \\
R7,1r+T4 & \vdash R8: id(A) * inv(id(A)) \neq id(A) \ \ \text{(Paramodulation)} \\
R4+R8 & \vdash R9: \Box
\end{array}
$$

11 Verwendung von Theorien: Semantische Ansätze: Theorieresolution

Die Theorieresolution ist ein Schema, um Information über die Bedeutung von Prädikaten- und Funktionssymbolen unmittelbar im (Resolutions-) Kalkül auszunutzen, indem man anstelle von Axiomen für diese Symbole maßgeschneiderte Schlußregeln verwendet. Sie wurde von Mark Stickel am SRI allgemein formuliert. Viele Spezialfälle davon, u.a. Paramodulation, waren jedoch schon vorher unter anderen Namen bekannt.

Z.B. ist es dadurch möglich, direkt mit arithmetischen Bedingungen umzugehen, die man ohne diese Technik nur direkt (und umständlich) in Prädikatenlogik kodieren kann.

Zur Motivation der Vorgehensweise erinnern wir uns an die Begründung für die Korrektheit der einfachen Resolutionsregel:

$$\begin{array}{ll} \text{Klausel1:} & L, K_1, \ldots, K_n \\ \text{Klausel2:} & \underline{\neg L, M_1, \ldots, M_m} \\ \text{Resolvente:} & K_1, \ldots, K_n, M_1, \ldots, M_m \end{array}$$

Das entscheidende Argument dafür, daß die Resolvente aus den Elternklauseln folgt, war: wenn eine Interpretation das Literal L erfüllt, dann falsifiziert sie $\neg L$. Wesentlich ist also, daß keine Interpretation sowohl L als auch $\neg L$ erfüllen kann. Diese Eigenschaft haben zwei Literale dann, wenn sie die rein syntaktische Bedingung erfüllen, komplementär zu sein, also übereinstimmende Prädikatensymbole und Termlisten, aber verschiedene Vorzeichen zu besitzen.

In vielen Fällen kann man den syntaktischen Komplementaritätsbegriff verallgemeinern, indem man ausnutzt, daß nicht völlig beliebige, sondern nur bestimmte Klassen von Interpretationen in Frage kommen. Zum Beispiel könnte eine Formelmenge geeignete Axiome für das Prädikatensymbol $<$ enthalten, so daß nur solche Interpretationen Modelle sein können, die dem Symbol $<$ eine strikte Ordnungsrelation auf dem Universum zuordnen. Aufgrund der Eigenschaften solcher Relationen kann keine derartige Interpretation sowohl $a < b$ als auch $b < a$ erfüllen. In dem genannten Kontext sind diese beiden Literale zwar nicht syntaktisch, aber sozusagen semantisch komplementär, und auch folgender Ableitungsschritt ist korrekt:

$$\begin{array}{ll} \text{Klausel1:} & a < b, K \\ \text{Klausel2:} & \underline{b < a, M} \\ \text{Resolvente:} & K, M \end{array}$$

Als weitere Verallgemeinerung können wir sogar die Beschränkung auf zwei Elternklauseln aufgeben. Keine Interpretation der genannten Klasse kann sowohl $a < b$ als auch $b < c$ als auch $c < a$ erfüllen. Damit kann man analog zur Begründung für die einfache Resolution, nur mit mehr Fallunterscheidungen, auch folgenden Schritt als korrekt nachweisen:

$$\begin{array}{ll} \text{Klausel1:} & a < b, K \\ \text{Klausel2:} & b < c, M \\ \text{Klausel3:} & \underline{c < a, N} \\ \text{Resolvente:} & K, M \end{array}$$

Die Idee ist also, von dem Spezialfall zweier syntaktisch komplementärer Resolutionsliterale überzugehen zu einer beliebigen Menge von Literalen, so daß keine Interpretation einer gegebenen Klasse alle diese Resolutionsliterale erfüllen kann. Die "Klasse von Interpretationen" wird durch den Theoriebegriff präzisiert.

Einer erfüllbaren Menge $\mathcal{A}$ von Formeln läßt sich in PL_1 eindeutig die Klasse $\mathcal{M}$ ihrer Modelle zuordnen, also von Interpretationen, die die Formeln wahr machen. Dieser Klasse von Interpretationen entspricht wiederum eindeutig eine (unendliche) maximale Menge $\mathcal{T}$ von Formeln, die von allen Interpretationen in $\mathcal{M}$ erfüllt werden. Die Formelmenge $\mathcal{T}$ ist maximal in dem Sinn, daß jede weitere Formel die Modellklasse $\mathcal{M}$ einschränkt, also von wenigstens einem Modell für $\mathcal{A}$ falsifiziert wird. Per definitionem ist $\mathcal{T}$ gerade die Menge der Folgerungen aus $\mathcal{A}$. In dieser Sichtweise enthalten $\mathcal{M}$ und $\mathcal{T}$ dieselbe Information, und beide werden oft als Theorie bezeichnet. Da verschiedene Formelmengen dieselben Modelle haben können, stellt ein gegebenes $\mathcal{A}$ nur eine Alternative dar, die Theorie zu definieren. Man nennt $\mathcal{A}$ auch eine Präsentation oder Axiomatisierung der Theorie.

Definition 11.1. (Theorien)

Für eine Formelmenge $\mathcal{A}$ ist: Theorie($\mathcal{A}$) = Menge aller Modelle von $\mathcal{A}$ $\sim$ Menge aller Formeln, die in allen Modellen von $\mathcal{A}$ gelten.

Sei $\mathcal{T}$ eine gegebene Theorie:

$\mathcal{T}$-erfüllbar:: *Eine Formel F ist $\mathcal{T}$-erfüllbar, falls es ein Modell von $\mathcal{T}$ gibt, das F erfüllt.*

$\mathcal{T}$-unerfüllbar:: *Eine Formel F ist $\mathcal{T}$-erfüllbar, falls es kein Modell von $\mathcal{T}$ gibt, das F erfüllt.*

$\mathcal{T}$-allgemeingültig: *Eine Formel F ist $\mathcal{T}$-allgemeingültig: falls F in allen Modellen von $\mathcal{T}$ gilt.*

$\mathcal{T}$-Folgerung $F \models_{\mathcal{T}} G$ *Falls G in allen $\mathcal{T}$-Modellen von F gilt.*