Kapitel III:
Die Gleichheitsrelation

1 Das Problem der Gleichheit

(Karl-Hans Bläsius, Hans Jürgen Ohlbach, Axel Präcklein)

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 einmal einen Gleichheitsbeweis geführt hat.

Beispiel: Der Beweis des folgenden Theorems zeigt, welche typischen Schwierigkeiten bei Gleichheitsbeweisen auftreten. Zu zeigen sei: Eine Gruppe mit $x^2 = 1$ ist kommutativ.

Die Axiome einer Gruppe mit einem zweistelligen Verknüpfungssymbol • und einer einstelligen Funktion i (Inverses) sind:

$\forall x,y,z$	$(x \bullet y) \bullet z = x \bullet (y \bullet z)$	(Assoziativität)
$\forall x$	$1 \bullet x = x$	(Links-Eins)
$\forall x$	$x \bullet 1 = x$	(Rechts-Eins)
$\forall x$	$i(x) \bullet x = 1$	(Links-Inverses)
$\forall x$	$x \bullet i(x) = 1$	(Rechts-Inverses)

Als zusätzliche Voraussetzung soll gelten

$\forall x$	$x \bullet x = 1$	(Voraussetzung)

Die Behauptung ist nun:

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

Ein Beweis dieses Satzes wird zum Beispiel durch folgende Gleichungskette geführt:

(1)	$x \bullet y$	$= (1 \bullet x) \bullet y$	(Links-Eins)
(2)		$= ((y \bullet y) \bullet x) \bullet y$	(Voraussetzung)
(3)		$= ((y \bullet y) \bullet x) \bullet (y \bullet 1)$	(Rechts-Eins)
(4)		$= ((y \bullet y) \bullet x) \bullet (y \bullet (x \bullet x))$	(Voraussetzung)
(5)		$= (y \bullet ((y \bullet x) \bullet (y \bullet x))) \bullet x$	(mehrmals Assoziativität)
(6)		$= (y \bullet 1) \bullet x$	(Voraussetzung)
(7)		$= y \bullet x$	(Rechts-Eins)

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

(3)	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$(1 \bullet x) \bullet (y \bullet 1)$	(Voraussetzung)
oder	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$((y \bullet y) \bullet x) \bullet (y \bullet (1 \bullet 1))$	(Links- oder Rechts-Eins)
oder	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$((y \bullet y) \bullet x) \bullet ((y \bullet 1) \bullet 1)$	(Rechts-Eins)
oder	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$((y \bullet y) \bullet x) \bullet ((1 \bullet y) \bullet 1)$	(Links-Eins)
oder	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$(y \bullet (y \bullet x)) \bullet (y \bullet 1)$	(Assoziativität)
oder	$((y \bullet y) \bullet x) \bullet (y \bullet 1)$	=	$((y \bullet y) \bullet x) \bullet (y \bullet (i(w) \bullet w))$	(Links-Inverses)

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.

1.1 Formalisierung der Gleichheit innerhalb der Prädikatenlogik

In PL1 kann das Gleichheitsprädikat nicht durch eine endliche Axiomenmenge formalisiert werden. Abhängig von den in der Formelmenge vorkommenden Symbolen wird stattdessen die benötigte Axiomenmenge durch Instantiierung eines Axiomenschemas gewonnen:

$\forall x$	$x = x$	(Reflexivität)
$\forall x,y$	$x = y \Rightarrow y = x$	(Symmetrie)
$\forall x,y,z$	$x = y \wedge y = z \Rightarrow x = z$	(Transitivität)

Für jedes Argument von jedem in der Formelmenge vorkommenden Funktionssymbol f wird ein Substitutionsaxiom folgender Form benötigt:

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

Für jedes Argument von jedem in der Formelmenge vorkommenden Prädikatensymbol P wird ein weiteres Substitutionsaxiom benötigt:

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

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 einem der bekannten Kalküle 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 (vgl. [Bun83]). 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 „=“ auf eine Relation mit den gewünschten Eigenschaften abgebildet wird. Für Herbrandinterpretationen liest sich das dann folgendermaßen:

Eine Herbrandinterpretation I einer Formelmenge $\mathcal{F}$ ist eine *E-Interpretation* (englisch Equality-Interpretation) wenn

a) für alle Terme t des Herbranduniversums von $\mathcal{F}$: $(t = t) \in I$.

b) für alle $L \in I$: falls L den Unterterm s enthält und $(s = t) \in I$
dann ist auch $L' \in I$, wobei L' aus L durch Ersetzen eines Vorkommens von s durch t entsteht.

Die zweite Bedingung besagt gerade, daß gleiche Terme ausgetauscht werden können, ohne den Wahrheitsgehalt von Atomen zu verändern.

Beispiel: Eine E-Interpretation für die Formeln P(a) und a=b ist:

$$\{a=a,\ b=b,\ a=b,\ b=a,\ P(a),\ P(b)\}.$$

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. Eine Menge $\mathcal{G}$ von Gleichungen spezifiziert nun eine Menge von E-Modellen. Alle weiteren Gleichungen, die in diesen Modellen wahr sind, ergeben die *Gleichheitstheorie* mit der *Axiomatisierung* $\mathcal{G}$.

1.2 Gleichheit als Teilproblem

Unser erstes Beispiel war ein reines Gleichheitsproblem. Das Gleichheitsprädikat war das einzige in der Formelmenge vorkommende Prädikatensymbol, und das Ziel bestand darin, zu zeigen, daß zwei Terme mit Hilfe der Gleichungen syntaktisch gleich gemacht werden können und damit zu beweisen, daß die Theoremgleichung in der von den Axiomgleichungen definierten Theorie gültig ist. Wenn zwei Terme selbst nicht gleich sind, lassen sich unter Umständen Instanzen finden, für die dann die Gleichheit gezeigt werden kann. Solche *Unifikationsprobleme* entstehen häufig als Teilprobleme im Verlauf eines Beweises. Wie das folgende Beispiel zeigt, reicht es dann im allgemeinen aber nicht aus, nur eine Lösung zu finden.

Beispiel: Es seien folgende Klauseln gegeben:

C1: $u < 2 \cdot u, \quad \neg \text{Positiv}(u)$

C2: $\neg v < v \cdot 2$

C3: $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Assoziativität)

C4: Positiv(2·2), Positiv(2·(2·2))

Diese Klauselmenge ist offensichtlich unerfüllbar. (Der Rechner weiß jedoch außer den Axiomen zunächst nichts über die Symblole „<“, „Positiv“ und „·“) Wir versuchen, die Unerfüllbarkeit zunächst mit Hilfe einer intuitiven Gleichheitstheorieresolution zu zeigen. Dazu müssen wir die Literale C1,1 und C2,1 unifizieren. Die Unifikation des ersten Termpaares u und v ergibt auf jeden Fall $v \leftarrow u$, so daß nach Anwendung dieser Komponente das zweite Termpaar 2·u und u·2 übrigbleibt. Die naheliegende Lösung $u \leftarrow 2$ nützt jedoch nichts, da die zugehörige Resolvente zwischen C1 und C2 die Klausel ¬Positiv(2) ergibt, die mit keiner weiteren Klausel resolviert werden kann. Wir brauchen andere Lösungen für die Gleichung (für das Unifikationsproblem) $2 \cdot u = u \cdot 2$. Mit Hilfe der Assoziativität C3 erhalten wir tatsächlich noch weitere Einsetzungen für u, zum Beispiel $u \leftarrow 2 \cdot 2$, aber auch $u \leftarrow 2 \cdot (2 \cdot 2)$ und alle möglichen weiteren Verschachtelungen von (2·2). Die ersten beiden sind in diesem Beispiel gerade die gesuchten. Sie ermöglichen die Ableitung der beiden neuen Resolventen {¬Positiv(2·2)} und {¬Positiv(2·(2·2))} mit denen die Klausel C4 in zwei Schritten zur leeren Klausel resolviert werden kann.

Die allgemeine Behandlung der Gleichheit manifestiert sich damit in zwei Problemtypen:

1. Gleichheitsprobleme:
   Zeige, daß eine gegebene Gleichung gilt, d.h. aus anderen Gleichungen ohne weitere Variableneinsetzungen folgt.

2. Unifikationsprobleme (Lösen von Gleichungen):
   Finde Einsetzungen für die Variablen einer gegebenen Gleichung, unter denen sie aus anderen Gleichungen folgt.

Der zweite Typ umfaßt die ganze Problematik der Struktur von Lösungsmengen: Gibt es allgemeinste Lösungen? Wenn ja, wieviele davon gibt es? Wenn nicht, lassen sie sich wenigstens approximieren (durch eine Folge von zunehmend allgemeineren Lösungen)? Findet ein gegebener Algorithmus einige Lösungen, „genügend“ viele Lösungen, alle Lösungen? Allerdings haben konkrete Algorithmen zur Behandlung des ersten Problems wiederum Unterprobleme des zweiten Typs zu lösen, so daß sich bei allgemein anwendbaren Verfahren in der Praxis keine klare Trennung zwischen den beiden Problemtypen ergibt.

Ein wichtiges theoretisches Resultat, das die Grenzen des Machbaren absteckt, betrifft die Unentscheidbarkeit des Wort- und Unifizierbarkeitsproblems:

- Unentscheidbarkeit des Wortproblems:
  Es gibt keinen Algorithmus, der jedes beliebige vorgegebene Gleichheitsproblem entscheidet.

- Unentscheidbarkeit des Unifizierbarkeitsproblems:
  Es gibt keinen Algorithmus, der jedes beliebige vorgegebene Unifikationsproblem entscheidet.

Für beide Problemtypen sind bestenfalls Algorithmen denkbar, die nur im positiven Fall mit

Erfolg terminieren, d.h. die Probleme sind semientscheidbar. Damit ist klar, daß allgemeine Gleichheits- bzw. Unifikationsprobleme nur durch Suchverfahren behandelt werden können. Unterprobleme dieser Art, die während einer Beweissuche auftreten und deren Bearbeitung eventuell nicht terminiert, können daher nicht isoliert gelöst werden, sondern deren Suchvorgang muß in den gesamten Suchprozeß integriert sein.

1.3 Teilgebiete der Gleichheitsbehandlung

Das gesamte Gebiet läßt sich grob in drei große Teilgebiete einteilen:

1. Allgemeine Gleichheitsverfahren

Hier werden spezielle Kalküle und Kontrollstrategien entwickelt, so daß beispielsweise Gleichheits- und Unifikationsprobleme als Unterprobleme behandelt oder Terme vereinfacht werden können. Die entwickelten Verfahren, die häufig auf Erweiterungen der Resolution beruhen, sind meist für beliebige Gleichheitstheorien anwendbar.

2. Unifikationstheorie

Die Unifikationstheorie befaßt sich mit Lösbarkeitsfragen für spezielle Gleichungstheorien und untersucht die Struktur der Lösungsmengen für Unifikationsprobleme.

Unter der Theorieunifikation faßt man alle Aktivitäten zusammen, die die Entwicklung von Unifikationsalgorithmen für spezielle Gleichungstheorien zum Ziel haben.

3. Termersetzungssysteme

Für eine eingeschränkte aber noch hinreichend interessante Klasse von Gleichheitstheorien reicht es aus, Gleichungen nur in einer bestimmten Richtung anzuwenden, zum Beispiel, um Terme zu vereinfachen und schließlich auf eine Normalform zu bringen. Solche einseitig anzuwendenden Gleichungen, wie beispielsweise die Idempotenz $f(x,x)=x$, bezeichnet man als Termersetzungsregeln und Mengen von diesen Gleichungen als Termersetzungssysteme. Die Untersuchungen auf diesem Gebiet beschäftigen sich mit den Eigenschaften und der Generierung von Termersetzungssystemen und wie man sie benutzen kann, um das Gleichheitsproblem zu lösen. Die zur Erzeugung von Termersetzungssystemen entwickelte Technik kann allerdings so erweitert werden, daß ein sehr mächtiges allgemeines Gleichheitsverfahren entsteht.

Die angesprochenen Teilgebiete werden in den folgenden Beiträgen ausführlicher behandelt.