UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR
THEORETISCHE INFORMATIK

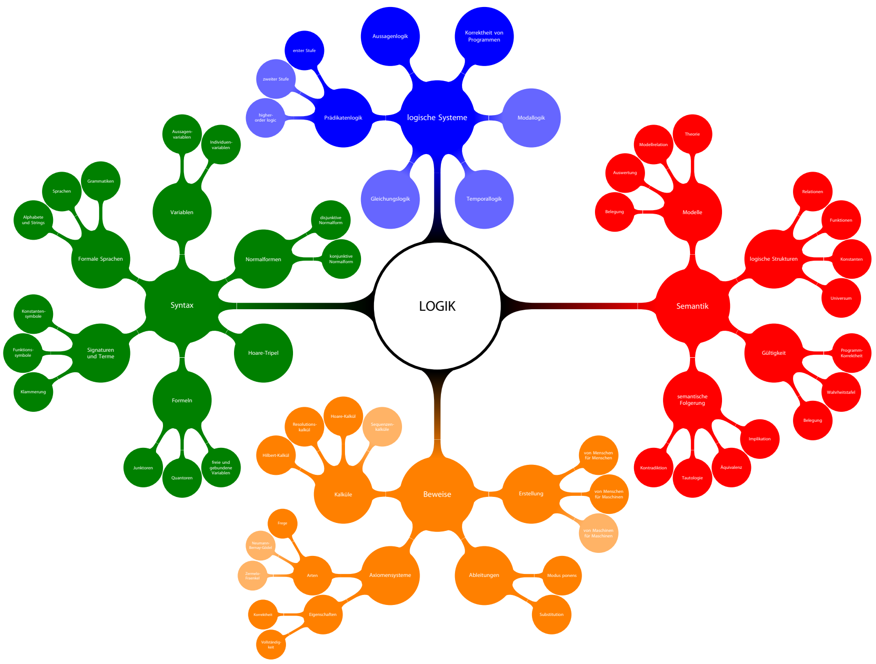
Vorlesungsskript

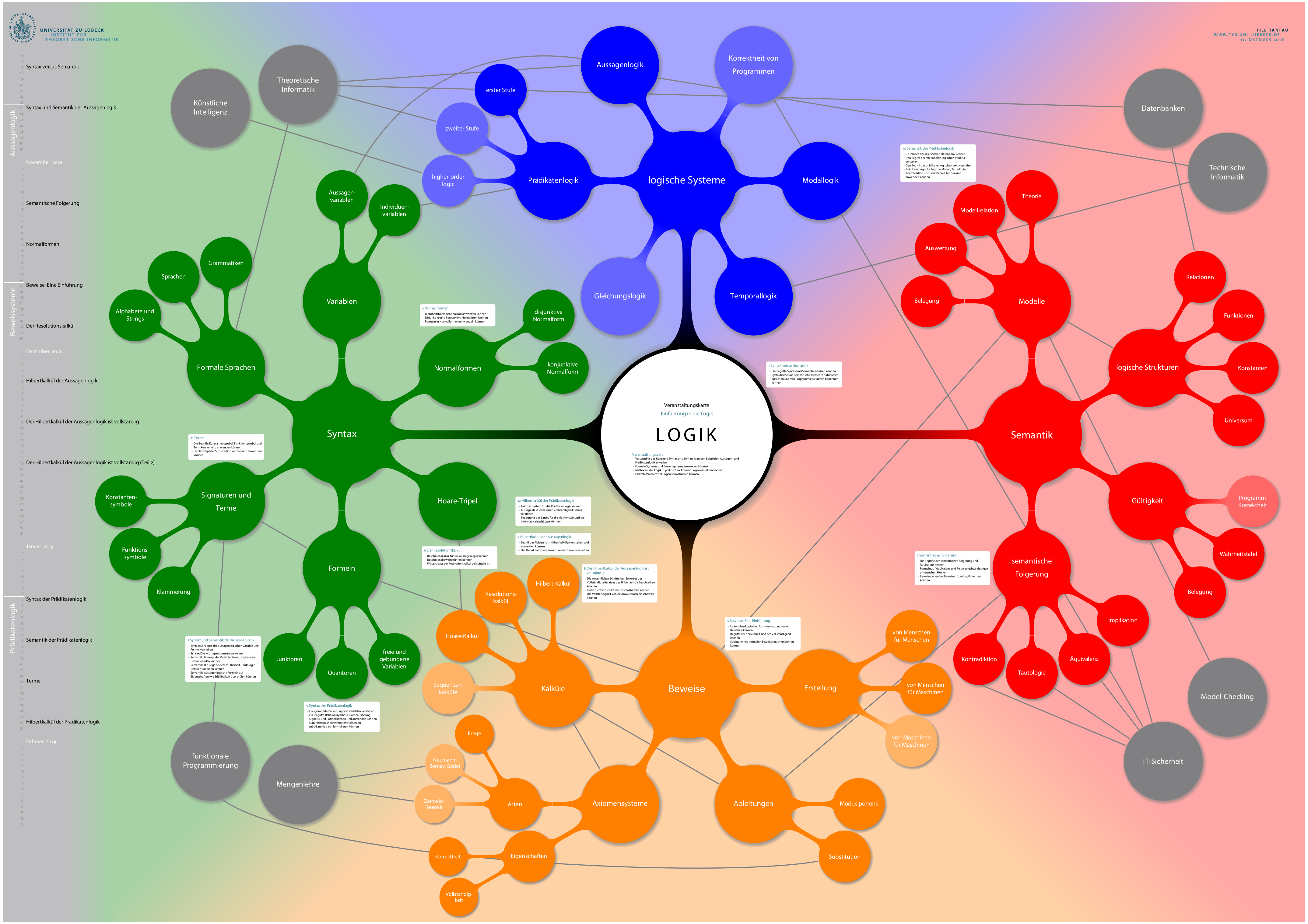
Einführung in die Logik

CS1002, Wintersemester 2017

Fassung vom 11. Oktober 2018

Till Tantau





UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR THEORETISCHE INFORMATIK
TILL TANTAU
WWW.TCS.UNI-LUEBECK.DE
11. OKTOBER 2018
Aussagenlogik
Syntax versus Semantik
Syntax und Semantik der Aussagenlogik
November 2018
Semantische Folgerung
Normalformen
Beweissysteme
Beweise: Eine Einführung
Der Resolutionskalkül
Dezember 2018
Hilbertkalkül der Aussagenlogik
Der Hilbertkalkül der Aussagenlogik ist vollständig
Der Hilbertkalkül der Aussagenlogik ist vollständig (Teil 2)
Januar 2019
Prädikatenlogik
Syntax der Prädikatenlogik
Semantik der Prädikatenlogik
Terme
Hilbertkalkül der Prädikatenlogik
Februar 2019
Veranstaltungskarte
Einführung in die Logik
LOGIK
Veranstaltungsziele
– Verständnis der Konzepte Syntax und Semantik an den Beispielen Aussagen- und Prädikatenlogik erwerben
– Formale Systeme und Beweissysteme anwenden können
– Methoden der Logik in praktischen Anwendungen einsetzen können
– Diskrete Problemstellungen formalisieren können
1 Syntax versus Semantik
– Die Begriffe Syntax und Semantik erklären können
– Syntaktische und semantische Elemente natürlicher Sprachen und von Programmiersprachen benennen können
2 Syntax und Semantik der Aussagenlogik
– Syntax: Konzepte der aussagenlogischen Variable und Formel verstehen
– Syntax: Die wichtigsten Junktoren kennen
– Semantik: Konzept der Variablenbelegung kennen und anwenden können
– Semantik: Die Begriffe der Erfüllbarkeit, Tautologie und Kontradiktion kennen
– Semantik: Aussagenlogische Formeln auf Eigenschaften wie Erfüllbarkeit überprüfen können
3 Semantische Folgerung
– Die Begriffe der semantischen Folgerung und Äquivalenz kennen
– Formeln auf Äquivalenz und Folgerungsbeziehungen untersuchen können
– Beweisebenen bei Beweisen über Logik trennen können
4 Normalformen
– Wahrheitstafeln kennen und anwenden können
– Disjunktive und konjunktive Normalform kennen
– Formeln in Normalformen umwandeln können
5 Beweise: Eine Einführung
– Unterschied zwischen formalen und normalen Beweisen kennen
– Begriffe der Korrektheit und der Vollständigkeit kennen
– Struktur eines normalen Beweises nachvollziehen können
6 Der Resolutionskalkül
– Resolutionskalkül für die Aussagenlogik kennen
– Resolutionsbeweise führen können
– Wissen, dass der Resolutionskalkül vollständig ist
7 Hilbertkalkül der Aussagenlogik
– Begriff der Ableitung in Hilbertkalkülen verstehen und anwenden können
– Das Deduktionstheorem und seinen Beweis verstehen
8 Der Hilbertkalkül der Aussagenlogik ist vollständig
– Die wesentlichen Schritte des Beweises des Vollständigkeitssatzes des Hilbertkalküls beschreiben können
– Einen nichtkonstruktiven Existenzbeweis kennen
– Die Vollständigkeit von Axiomsystemen einschätzen können
9 Syntax der Prädikatenlogik
– Die geänderte Bedeutung von Variablen verstehen
– Die Begriffe Relationssymbol, Quantor, Bindung, Signatur und Formel kennen und anwenden können
– Natürlichsprachliche Problemstellungen prädikatenlogisch formulieren können
10 Semantik der Prädikatenlogik
– Grundidee der relationalen Datenbank kennen
– Den Begriff der relationalen logischen Struktur verstehen
– Den Begriff der prädikatenlogischen Welt verstehen
– Prädikatenlogische Begriffe Modell, Tautologie, Kontradiktion und Erfüllbarkeit kennen und anwenden können
11 Terme
– Die Begriffe Konstantensymbol, Funktionssymbol und Term kennen und anwenden können
– Das Konzept der Substitution kennen und anwenden können
12 Hilbertkalkül der Prädikatenlogik
– Axiomensystem für die Prädikatenlogik kennen
– Aussage des Gödel'schen Vollständigkeitssatzes verstehen
– Bedeutung des Satzes für die Mathematik und die Informatik einschätzen können
logische Systeme
Aussagenlogik
Korrektheit von Programmen
Prädikatenlogik
erster Stufe
zweiter Stufe
higher-order logic
Modallogik
Gleichungslogik
Temporallogik
Syntax
Variablen
Aussagen-variablen
Individuen-variablen
Formale Sprachen
Sprachen
Grammatiken
Alphabete und Strings
Normalformen
disjunktive Normalform
konjunktive Normalform
Signaturen und Terme
Konstanten-symbole
Funktions-symbole
Klammerung
Hoare-Tripel
Formeln
Junktoren
Quantoren
freie und gebundene Variablen
Semantik
Modelle
Theorie
Modellrelation
Auswertung
Belegung
logische Strukturen
Relationen
Funktionen
Konstanten
Universum
Gültigkeit
Programm-Korrektheit
Wahrheitstafel
Belegung
semantische Folgerung
Implikation
Äquivalenz
Tautologie
Kontradiktion
Beweise
Kalküle
Hilbert-Kalkül
Resolutions-kalkül
Hoare-Kalkül
Sequenzen-kalküle
Erstellung
von Menschen für Menschen
von Menschen für Maschinen
von Maschinen für Maschinen
Axiomensysteme
Arten
Frege
Neumann-Bernay-Gödel
Zermelo-Fraenkel
Eigenschaften
Korrektheit
Vollständig-keit
Ableitungen
Modus ponens
Substitution
Theoretische Informatik
Künstliche Intelligenz
funktionale Programmierung
Mengenlehre
Datenbanken
Technische Informatik
Model-Checking
IT-Sicherheit

Inhaltsverzeichnis

Vorwort

Zur Einstimmung drei Zitate:

> *Der folgende Satz ist falsch. Der vorherige Satz ist richtig.*
>
> *Niemand hat die Absicht, eine Mauer zu bauen.*
>
> *Ein Kreter sagt: »Alle Kreter lügen.«*

Was ist *wahr*, was ist *falsch*? Dies ist die zentrale Frage, um die sich diese Veranstaltung drehen wird. Um es gleich vorwegzunehmen: Das erste Zitat werden wir als *kontradiktorisch* entlarven, beim zweiten Satz hat Walter Ulbricht einfach glatt gelogen, über den dritten dürfen Sie selbst erstmal ein wenig nachdenken. Ebenfalls gleich vorweg die große Enttäuschung: Wirklich *lösen* werden wir die Frage »Was ist Wahrheit?« nicht im Rahmen dieser Verstaltung. Die Philosophie ringt mit ihr schon buchstäblich seit Jahrtausenden, ohne sie endgültig beantwortet zu haben.

Aus diesem Grund – und auch weil Sie ja eher Informatik studieren und weniger Philosophie – wird es in dieser Veranstaltung weniger um die tiefen philosophische Probleme gehen, über die man in der Logik praktisch schon mit den ersten Schritten stolpert. Stattdessen backen wir kleinere Brötchen, die für Sie in ihrem späteren Beruf – sei es als Software-Entwickler oder Informatik-Forscherin – nahrhafter sein werden. Zunächst werden Sie die zwei Grundbegriffe »Syntax« und »Semantik« kennen lernen, welche in der Informatik auch außerhalb der klassichen Logik immer wieder auftauchen werden. Dann wird es ausführlich um die sogenannte »Aussagenlogik« gehen, welche sowohl beim Programmieren wie auch beim Chip-Design ständig benötigt wird. Wir werden auch die sogenannten »Prädikatenlogik« behandeln, welche sehr nützlich ist, wenn man beschreiben möchte, was ein Programm eigentlich machen *sollte* (was erfahrungsgemäß nie das ist, was das Programm dann tatsächlich macht). Einiges von dem, was Sie in dieser Veranstaltung lernen werden, wird für Sie im späteren Leben sehr nützlich sein – anderes überhaupt nicht.

Soviel ganz kurz zum Inhalt der Veranstaltung; nun zu den Zielen. Jedes Kapitel dieses Skripts entspricht einer Vorlesungsdoppelstunde und mit jedem Kapitel verfolge ich gewisse Ziele, welche Sie am Anfang des jeweiligen Kapitels genannt finden. Neben diesen etwas kleinteiligen Zielen gibt es auch folgende zentralen »offiziellen« Veranstaltungsziele, wie sie auch im Modulhandbuch zu finden sind:

1. Verständnis der Konzepte Syntax und Semantik an den Beispielen Aussagen- und Prädikatenlogik erwerben
2. Formale Systeme und Beweissysteme anwenden können
3. Methoden der Logik in praktischen Anwendungen einsetzen können
4. Diskrete Problemstellungen formalisieren können

Was dies alles genau bedeutet, wird während der Veranstaltung (hoffentlich) noch klarer werden. (Oder könnten Sie sofort sagen, was genau eine »diskrete Problemstellung« ist? Jedenfalls nicht das Gegenteil einer »indiskreten Antwort«.) Jedoch können Sie an den Zielen jetzt schon ablesen, dass es nicht nur um Logik im klassischen Sinne gehen wird. Sie werden auch lernen »Konzepte zu formalieren«, was die vornehme Formulierung ist von »Dinge so aufzuschreiben, dass ein Computer sie versteht«.

Die Wörtchen »können« taucht bei den Veranstaltungszielen recht häufig auf. Um etwas wirklich zu können, reicht es nicht, davon gehört zu haben oder davon gelesen zu haben. Man muss es auch wirklich *getan* haben: Sie können sich tausend Fußballspiele im Fernsehen anschauen, sie sind deshalb noch kein guter Fußballspieler; sie können tausend Stunden

World of Warcraft spielen, sie werden deshalb trotzdem keinen Frostblitz auf Ihren Professor geschleudert bekommen.

Deshalb steht bei dieser Veranstaltung der Übungsbetrieb mindestens gleichberechtigt neben der Vorlesung. Der Ablauf ist dabei folgender: In der Vorlesung werde ich Ihnen die Thematik vorstellen und Sie können schon mit dem Üben im Rahmen kleiner Miniübungen *während der Vorlesung* beginnen. Jede Woche gibt es ein Übungsblatt, das inhaltlich zu den Vorlesung gehört. Sie müssen sich die Übungsblätter aber nicht »alleine erkämpfen«. Vielmehr gibt es Tutorien, in denen Sie Aufgaben üben werden, die »so ähnlich« wie die Aufgaben auf den Übungsblättern sind. Sie werden feststellen, dass die als »leicht« und in der Regel auch die als »mittel« eingestuften Aufgaben mit der Vorbereitung im Tutorium in der Tat mit vertretbarem Aufwand schaffbar sind. Ist eine Aufgabe »schwer«, so ist es kein Unglück, wenn Sie diese nicht schaffen – probieren sollten Sie es aber trotzdem.

Ich wünsche Ihnen viel Spaß mit dieser Veranstaltung.

Till Tantau

Teil I

Der Begriff der Syntax

Hier ein paar Vorurteile über einige europäische Länder und ihren Umgang mit Regeln: In England ist alles erlaubt, außer was explizit verboten ist. In Deutschland ist alles verboten, außer was explizit erlaubt ist. In Italien ist alles erlaubt, auch was explizit verboten ist. Und in Russland ist alles verboten, auch was explizit erlaubt ist. (Je nach eigenen Sym- und Antipathien können Sie natürlich gerne Länder munter substituieren.)

Wie verhält es sich nun mit Computern, welchem »Regelungssystem« neigen sie zu? Vielleicht weil der erste Computer, die Z1, in Deutschland gebaut wurde, dem »deutschen«: Computer sind geradezu vernarrt in Regeln – und wenn nicht auch die abstruseste Ausführungsvorschrift penibelst eingehalten wird, wird dies sofort mit »schweren Schutzverletzungen« oder banaler mit einem »Syntax-Error« quittiert. Es grenzt manchmal schon an Arbeitsverweigerung, wenn Ihnen mitgeteilt wird, dass »dieser lange und komplexe Befehl zwar perfekt verstanden wurde und auch ohne Weiteres ausgeführt werden könnte, dass aber laut Grammatikregeln aus der Vorschrift ISO/IEC 14882:2003 das letzte Zeichen des Befehls ein Semikolon hätte sein müssen, weshalb dies nun nicht geschieht, und die Arbeit der letzten Stunden vernichtet wurde. Hochachtungsvoll, Ihr Compiler.« Verglichen mit der bei typischen Programmiersprachen nötigen Akribie ist jedes Steuererklärungsformular ein anarchistisches Pamphlet.

Computer brauchen für ihre Arbeit ständig umfangreiche Regelwerke. Diese legen fest, was erlaubt ist und was nicht. Das Regelwerk für die Programmiersprache Java beispielsweise enthält genaueste Regeln darüber, ob man nun »`if`« oder auch »`If`« schreiben muss, wenn man »Wenn-Dann« meint. Es gibt Regeln, wie Programme mit dem Betriebssystem kommunizieren dürfen oder gar mit anderen Computern. Wenn Ihr Computer einem anderen Computer ein sogenanntes TCP/IP-Paket schickt, dann muss ein ganzes Buch an Regeln eingehalten werden, damit dieses auch ankommt.

Mit dem Begriff *Syntax* bezeichnen wir allgemein solche Regelwerke. Die Syntax einer Programmiersprache legt alles fest, was der Compiler überprüft. Die Syntax eines Kommunikationsprotokolls legt alles fest, was nötig ist, damit man »einander versteht«. Die Syntax einer Logik legt fest, welche Formeln erlaubt sind und welche nicht.

1-1

Kapitel 1

Syntax versus Semantik

Text und seine Bedeutung

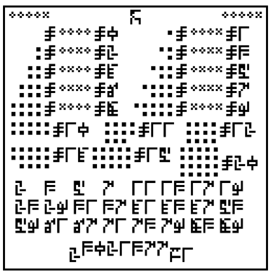
1-2

Lernziele dieses Kapitels

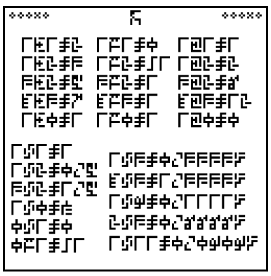
1. Die Begriffe Syntax und Semantik erklären können
2. Syntaktische und semantische Elemente natürlicher Sprachen und von Programmiersprachen benennen können

Inhalte dieses Kapitels

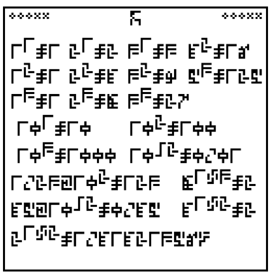
Worum es heute geht



Public domain



Public domain



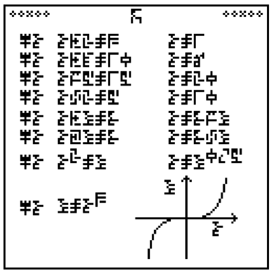
Public domain

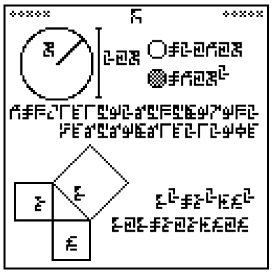
Am Rand sehen Sie die ersten Tafeln einer außerirdischen Nachricht. Ja, Sie haben richtig gelesen, einer *außerirdische Nachricht*. Allerdings nicht *von* Außerirdischen, sondern *an* Außerirdische. Diese Nachricht wird seit 1999 verschickt in der Hoffnung, dass Außerirdische sie lesen, verstehen und antworten. Die Kommunikation mit Außerirdischen, die noch nicht auf der Erde vorbeigeschaut haben, ist etwas kniffelig, denn schließlich wird man nicht annehmen können, dass diese, sagen wir, Englisch oder XML sprechen. Deshalb hat man die Tafeln so angelegt, dass sie völlig selbsterklärend sind – zumindest für einigermaßen gebildete Lebensformen, die einen soliden mathematisch-naturwissenschaftlichen Unterricht der Sekundarstufe II genossen haben.

Als kleiner Test, ob Außerirdische die Nachricht verstehen werden, stellen Sie sich bitte kurz vor, Sie seien ein Außerirdischer und erhielten diese Nachricht. (Sollten Sie sich sowieso generell für einen Außerirdischen halten, um so besser.) Was könnten die Menschen mit dem Text gemeint haben?

Zunächst fällt ins Auge (sollten Sie ein Auge besitzen), dass der Text irgendwie strukturiert ist. Da gibt es Ansammlungen von schwarzen Punkten und große Flächen von weißen Punkten. Nennen wir die Ansammlungen von schwarzen Punkten doch vorübergehend »Symbole«. Diese Symbole scheinen grob in einem Raster angeordnet zu sein, jedenfalls nicht völlig zufällig. Auch fällt auf, dass sich manche Symbole wiederholen und dass manche zu größeren Gruppen, nennen wir doch »Zeilen«, gruppiert sind.

Solche Beobachtungen sind *syntaktischer* Natur, wir haben etwas über die *Syntax* herausgefunden, die von den Absendern der Nachricht benutzt wurde. Das heißt noch nicht, dass wir die *Semantik*, also die *Bedeutung*, der Nachricht bereits erkannt haben.





Um etwas über die Bedeutung herauszufinden, müssen Sie kreativ werden. In der ersten Tafel fällt auf, dass im oberen Teil Ansammlungen von dicken Punkten in der Nähe von bestimmten Symbolen stehen. Nehmen wir vorübergehend an, dass diese Symbole Abkürzungen für die *Anzahlen* der Punkte sind. Diese These über die *Semantik* der Symbole hält dann auch einer eingehenderen Betrachtung statt.

Wer genügend Science-Fiction-Romane gelesen hat, weiß natürlich, dass bei Nachrichten an Außerirdische früher oder später Primzahlen ins Spiel kommen. Und tatsächlich, im unteren Teil der ersten Tafel finden sich nacheinander die Zahlen 2, 3, 5, 7, 11, 13 und so weiter. Am Ende der ersten Tafel findet sich dann noch 2 gefolgt etwas höher stehend 3021377 gefolgt von einem neuen, unbekannten Symbol, gefolgt von einer 1. Wenn Sie es nicht schon erkannt haben, dann können Sie ja mal über die Semantik der syntaktischen Konstrukte »etwas höher stehend« und dem neuen, unbekannten Symbol nachdenken.

Kehren Sie nun bitte auf die Erde zurück. In diesem Kapitel soll der Unterschied zwischen Syntax und Semantik an etwas bodenständigeren Beispielen aus der Informatik und der Logik herausgearbeitet werden; jedoch werden Sie sehen, dass das Prinzip genau dasselbe wie bei der Nachricht an die Außerirdischen ist: Die Syntax regelt, was man alles prinzipiell hinschreiben darf, die Semantik regelt, was das dann bedeutet.

1.1 Was ist Syntax?

Die zwei Hauptbegriffe der heutigen Vorlesung. 1-4

Grobe Definition
Unter einer *Syntax* verstehen wir *Regeln* nach denen Texte *strukturiert* werden (Grammatik).

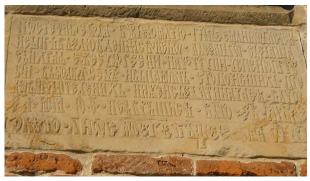
Grobe Definition
Unter einer *Semantik* verstehen wir die Zuordnung von *Bedeutung* zu Texten.

1.1.1 Syntax natürlicher Sprachen

Beobachtungen zu einem ägyptischen Text. 1-5

Beobachtungen
Wir haben keine Ahnung, was der Text bedeutet. Es gibt aber *Regeln*, die offenbar eingehalten wurden, wie »Hieroglyphen stehen in Zeilen«. Solche Regeln sind *syntaktische Regeln* – man kann sie überprüfen, ohne den Inhalt zu verstehen.

Beobachtungen zu einem kyrillischen Text. 1-6



Beobachtungen
Wir haben wieder keine Ahnung, was der Text bedeutet. Es gibt aber *Regeln*, die offenbar eingehalten wurden, und wir kennen mehr Regeln als bei den Hieroglyphen.

✎ **Zur Diskussion**
Welche syntaktischen Regeln fallen Ihnen ein, die bei dem Text eingehalten wurden?

Beobachtungen zu einem deutschen Text. 1-7

> Informatiker lieben Logiker.

Beobachtungen
Auch hier werden viele syntaktische Regeln eingehalten. Es fällt uns aber *schwerer*, diese zu erkennen. Der Grund ist, dass wir *sofort über die Bedeutung nachdenken*.

Zur Syntax von natürlichen Sprachen. 1-8
Die *Syntax* einer natürlichen Sprache ist die Menge an *Regeln*, nach denen Sätze gebildet werden dürfen. Die *Bedeutung* oder der *Sinn* der gebildeten Sätze ist dabei unerheblich. Jede Sprache hat ihre eigene Syntax; die Syntax verschiedener Sprachen ähneln sich aber oft. Dabei ist es nicht immer klar, ob eine Regel noch zur Syntax gehört oder ob es schon um den Sinn geht.
Beispiel: Substantive werden groß geschrieben.

1.1.2 Syntax von Programmiersprachen

1-9 **Beobachtungen zu einem Programmtext.**

```
\def\pgfpointadd#1#2{%
  \pgf@process{#1}%
  \pgf@xa=\pgf@x%
  \pgf@ya=\pgf@y%
  \pgf@process{#2}%
  \advance\pgf@x by\pgf@xa%
  \advance\pgf@y by\pgf@ya}
```

Beobachtungen
Der Programmtext sieht sehr kryptisch aus. Trotzdem gibt es offenbar wieder Regeln. So scheint einem Doppelkreuz eine Ziffer zu folgen und Zeilen muss man offenbar mit Prozentzeichen beenden.

1-10 **Beobachtungen zu einem weiteren Programmtext.**

```
for (int i = 0; i < 100; i++)
  a[i] = a[i];
```

Beobachtungen
Wieder gibt es Regeln, die eingehalten werden, und wieder fällt es uns *schwerer*, diese zu erkennen, da wir *sofort über den Sinn nachdenken*.

1-11 Zur Syntax von Programmiersprachen
Die *Syntax* einer Programmiersprache ist die *Menge von Regeln* nach der Programmtexte gebildet werden dürfen. Die *Bedeutung* oder der *Sinn* der Programmtexte ist dabei egal. Jede Programmiersprache hat ihre eigene Syntax; die Syntax verschiedener Sprachen ähneln sich aber oft.

1-12 ✎ Zur Übung
Welche der folgenden Regeln sind Syntax-Regeln?

1. Bezeichner dürfen nicht mit einer Ziffer anfangen.
2. Programme müssen in endlicher Zeit ein Ergebnis produzieren.
3. Öffnende und schließende geschweifte Klammern müssen »balanciert« sein.
4. Methoden von Null-Objekten dürfen nicht aufgerufen werden.
5. Variablen müssen vor ihrer ersten Benutzung deklariert werden.

1.1.3 Syntax logischer Sprachen

1-13 **Beobachtungen zu einer logischen Formel.**

$$p \to q \wedge \neg q$$

Beobachtungen
Auch logische Formeln haben eine syntaktische Struktur. So wäre es *syntaktisch falsch,* statt einem Pfeil zwei Pfeile zu benutzen. Es wäre aber *syntaktisch richtig,* statt einem Negationszeichen zwei Negationszeichen zu verwenden.

1-14 Zur Syntax von logischen Sprachen
Die *Syntax* einer logischen Sprache ist die *Menge von Regeln,* nach der Formeln gebildet werden dürfen. Die *Bedeutung* oder der *Sinn* der Formeln ist dabei egal. Jede logische Sprache hat ihre eigene Syntax; die Syntax verschiedener Sprachen ähneln sich aber oft.

1.2 Was ist Semantik?

1.2.1 Semantik natürlicher Sprachen

Was bedeutet ein Satz? 1-15

Steter Tropfen höhlt den Stein.

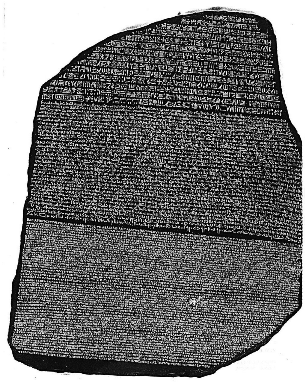
Dieser Satz hat eine *Bedeutung*, die eine *Semantik* festlegt. Ein Satz kann dabei *mehrere Bedeutungen haben*, welche durch *unterschiedliche Semantiken* gegeben sind:

- In der *wortwörtlichen Semantik* sagt der Satz aus, dass Steine ausgehöhlt werden, wenn man jahrelang Wasser auf sie tropft.
- In der *übertragenen Semantik* sagt der Satz aus, dass sich Beharrlichkeit auszahlt.

Syntaktisch falschen Sätzen wird im Allgemeinen keine Bedeutung zugewiesen.

Die Semantik der Hieroglyphen 1-16

Dreimal eine unterschiedliche Syntax – eine Semantik.



Unknown author, public domain.

1.2.2 Semantik von Programmiersprachen

Was bedeutet ein Programm? 1-17

```
for (int i = 0; i < 100; i++)
  a[i] = a[i];
```

Auch dieser Programmtext »bedeutet etwas«, wir »meinen etwas« mit diesem Text. Die *Semantik der Programmiersprache* legt fest, was mit dem Programmtext gemeint ist. Er kann *mehrere Bedeutungen haben*, welche durch *unterschiedliche Semantiken* gegeben sind:

- In der *operationalen Semantik* bedeutet der Programmtext, dass die ersten einhundert Elemente eines Arrays a nacheinander ihren eigenen Wert zugewiesen bekommen.
- In der *denotationellen Semantik* bedeutet der Programmtext, dass nichts passiert.

Zusammenfassung dieses Kapitels

► Syntax versus Semantik 1-19

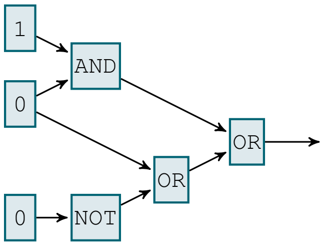
Eine *Syntax* beschreibt, wie Texte aufgebaut sein dürfen. Eine *Semantik* beschreibt, was Texte *bedeuten*.

Übungen zu diesem Kapitel

Übung 1.1 Kodieren üben, mittel

Ein *Schaltkreis* besteht aus Gattern und Verbindungen. Es gibt fünf Arten von Gattern: `0`, `1`, `AND`, `OR`, `NOT`. Alle Gatter haben einen Ausgang. Die Gatter `0` und `1` haben keinen Eingang, das Gatter `NOT` hat einen Eingang, die Gatter `AND` und `OR` haben zwei Eingänge. Bei jedem Gatter muss jeder Eingange mit dem Ausgang eines anderen Gatters verbunden sein.

Überlegen Sie sich eine Methode, um Schaltkreise als Unicode-Strings zu kodieren. Beschreiben Sie Ihre Methode und kodieren Sie den unten abgebildeten Schaltkreis damit.



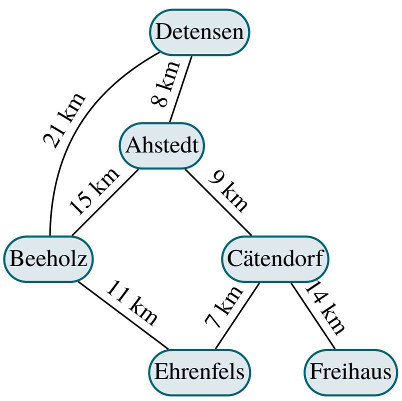
Übung 1.2 Kodieren üben, mittel

Wer kennt das nicht: Man fährt mit seinem nagelneuen Off-Roader in die Pampa und das Navigationssystem meldet

> »Bitte wenden!«

Der Navi kennt wieder einmal das lokale Straßennetz nicht, weshalb wir spontan beschließen, unser eigenes System zu programmieren. Gesagt, getan. Die erste Aufgabe ist, die Straßenkarte unserem System zur Verfügung zu stellen. Dabei betrachten wir das Straßennetz als ungerichteten Graphen mit den Städten als Knoten und den Straßen als Kanten.

Überlegen Sie sich eine Methode, um ungerichtete Graphen als Unicode-String zu kodieren. Beschreiben Sie Ihre Methode und kodieren Sie das unten stehende Straßennetz damit.



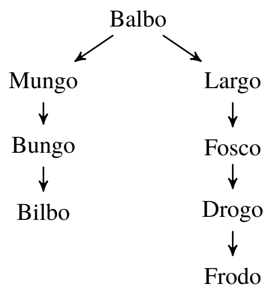
Übung 1.3 Kodieren üben, mittel

Bevor Bilbo Beutlin mit Thorin, Bifur, Bofur, Fili, Kili, Dori, Nori, Ori, Oin, Gloin, Balin, Dwalin und Bombur zum Einsamen Berg in Rhovanion aufbricht, um gegen den Drachen Smaug anzutreten, erhält er von Gandalf eine Karte von Mittelerde. Da Gandalf ein mächtiger Zauberer ist, hat er die Karte mit Ti*k*Z kodiert. Helfen Sie Bilbo diese Karte zu dekodieren und fertigen Sie eine Skizze von Mittelerde an.

```
\tikz \graph [no placement] {
  Mordor      [x=2, y=0];
  Gondor      [x=0, y=0];
  Rohan       [x=1, y=1];
  Rhovanion   [x=1, y=2];
  Eriador     [x=-1,y=2];
  Forodwaith [x=0, y=3];
  Eriador     -- Rhovanion;
  Eriador     -- Gondor;
  Eriador     -- Rohan;
  Forodwaith -- Rhovanion;
  Gondor      -- Rohan;
  Mordor      -- Rohan;
  Rhovanion   -- Rohan;
};
```

Übung 1.4 Kodieren üben, mittel

Überlegen Sie sich eine Methode, um Bäume möglichst kompakt als Unicode-String zu kodieren. Beschreiben Sie Ihre Methode und kodieren Sie den folgenden Ausschnitt aus Bilbo Beutlins Stammbaum damit. Geben Sie das benutzte Alphabet an.



Teil II

Aussagenlogik

Die Grundideen der Aussagenlogik werden Sie in dieser Veranstaltung nicht erlernen – die sind Ihnen nämlich angeboren! Man braucht kein Hochschulstudium, um aus »der Weihnachtsmann hat einen roten Mantel« und »Sophie hat keinen roten Mantel« messerscharf zu schließen »Sophie ist nicht der Weihnachtsmann«. Viele der Grundregeln der Aussagenlogik sind uns tatsächlich als »gesunder Menschenverstand« geläufig, weshalb sich die Aussagenlogik als die erste Logik, die wir untersuchen werden, gut anbietet.

Irritierend stimmt an dieser Stelle vielleicht, dass es in Form der Aussagenlogik überhaupt eine bestimmte *Art* von Logik geben soll. Wieso wird »die Logik« getrennt in Aussagenlogik, Prädikatenlogik, Modallogik, Temporallogik und viele mehr? Jede untersucht einen anderen Aspekt logischer Schlüsse besonders intensiv. Bei der Aussagenlogik geht es, wie der Name schon sagt, besonders um die logischen Zusammenhänge zwischen *Aussagen*; bei der Prädikatenlogik geht es um *Prädikate* (was immer diese sein mögen, wir klären das später noch); bei der Temporallogik geht es um *zeitliche Abfolgen* und so weiter. Ganz getrennt sind diese »Logiken« aber nicht, fortgeschrittene benutzen den Grundstock der Aussagenlogik und oft auch die Prädikatenlogik ganz selbstverständlich.

Was sind nun aber die »Aussagen«, um die es in der Aussageblogik geht? Eine offizielle Definition lautet: »Aussagen sind Sätze, denen als ganzes eindeutig einer der Wahrheitswerte *wahr* oder *falsch* zugewiesen werden kann.« Beispielsweise ist der Satz »Die Erde ist ein Planet« eine wahre Aussage, wohingegen »Der Mond ist grün« eine falsche ist und »Dieses Bild ist hässlich« gar keine Aussage im Sinne der Aussagenlogik ist, da man schwerlich einen eindeutigen Wahrheitswert wird zuordnen können. Schönheit liegt bekanntlich im Auge des Betrachters.

Wenn man etwas darüber nachdenkt, ob bestimmte Sätze Aussagen sind oder nicht, so stellt man schnell fest, dass dies ein verymintes Feld ist. Ständig begegnen einem Sätze wie »Berlin ist die Hauptstadt von Deutschland«. Hatte die Aussage 1980 einen anderen Wahrheitswert? War sie im Jahr 800 überhaupt eine Aussage? Bei Sätzen wie »Gott ist tot« streiten sich ganze Wissenschaftsdisziplinen (Linguistik, Physik, Religion und Philosophie) leidenschaftlich um die Frage, ob es sich um eine Aussage handelt (Linguist: »ja«, Physiker: »nein«, Priester: »ja, aber sie stimmt nicht«, Philosoph: »ja und sie stimmt«).

Wie schon im Vorwort erwähnt, soll es in dieser Veranstaltung nicht um tiefe philosophische Fragen gehen. Vielmehr werden wir einen Trick verwenden, den Mathematiker häufig anwenden: Wir *abstrahieren* einfach von all den praktischen und konkreten Problemen und benutzen Variablen für Aussagen. Den Vorgang, die Wirklichkeit zu ignorieren und sich stattdessen eine »saubere« mathematisch beherrschbare Welt zu schaffen, bezeichnet man beschönigend als *Formalisieren*. Mit anderen Worten: In der *mathematischen Logik* werden wir uns eine völlig eigene Welt schaffen, die logische Zusammenhänge aus der Wirklichkeit nur sehr bedingt korrekt abbilden.

2-1

Kapitel 2
Syntax und Semantik der Aussagenlogik
Aufbruch zu neuen Welten

2-2

Lernziele dieses Kapitels

1. Syntax: Konzepte der aussagenlogischen Variable und Formel verstehen
2. Syntax: Die wichtigsten Junktoren kennen
3. Semantik: Konzept der Variablenbelegung kennen und anwenden können
4. Semantik: Die Begriffe der Erfüllbarkeit, Tautologie und Kontradiktion kennen
5. Semantik: Aussagenlogische Formeln auf Eigenschaften wie Erfüllbarkeit überprüfen können

Inhalte dieses Kapitels

Worum es heute geht

Chefinspektor Clouseau hat wieder einen neuen Fall: Es ist mal wieder ein Juwel geraubt worden. Aus zuverlässiger Quelle hat der Inspektor (Verzeihung, Chefinspektor) erfahren, dass drei Personen als Diebe in Frage kommen: Alice, Bob und Charly, vielleicht sogar mehrere von ihnen. Die Ermittlungen von Kommisar Dreyfus ergeben Folgendes:

1. Ohne Charly würde Bob nie einen Einbruch begehen.
2. Alice hingegen kann Charly nicht ausstehen und würde nie mit ihm zusammen ein Ding drehen.
3. Ein Zeuge ist sich sicher, Bob oder Charly zur Tatzeit in einem pittoresken Lokal einen Cappuccino schlürfen gesehen zu haben; der Zeuge kann sich aber nicht erinnern, welchen von beiden.
4. Auf einem Überwachungsvideo ist klar zu sehen, dass mindestens ein Täter mit Glatze an dem Diebstahl beteiligt war.

Wen sollte Chefinspektor Clousseau daraufhin alles verhaften lassen? (Dies ist übrigens eine ganz andere Frage als, wen er tatsächlich verhaften wird. Wie Kommisar Dreyfus Ihnen ausführlich würde bestätigen können, folgt die Logik des Chefinspektors ihren ganz eigenen Regeln.)

In der Aussagenlogik geht es darum, solche Fragen zu klären, indem die Beziehungen zwischen *Aussagen* systematisch untersucht werden. Bei dem obigen Beispiel gibt es drei Aussagen, die wahr oder falsch sein können und die in Beziehung gesetzt werden: Die erste lautet »Alice war beteiligt«, die zweite »Bob war beteiligt« und die dritte »Charly war beteiligt«. Wirklich spannend ist nun die Frage, wie diese Aussagen mittel *Junktoren* wie »und«,

»oder«, »nicht« oder auch »wenn, dann« verbunden sind. Solche durch die Verbindung mehrerer Aussagen entstandenen Sätze nennen wir originellerweise *Formeln*, auch wenn hier überhaupt nicht gerechnet wird.

Wie sollte man Formeln aufschreiben? Mathematiker und Informatiker hegen allgemein eine gewisse Antipathie gegen einfache, verständliche Notationen, weshalb Sie in der Aussagenlogik statt »ein Zeuge ist sich sicher, Bob oder Charly zur Tatzeit in einem pittoresken Lokal einen Cappuccino schlürfen gesehen zu haben, kann sich aber nicht erinnern wen« schreiben müssen »$\neg(b \wedge c)$«, in Java hingegen »`!(b && c)`«. Fairerweise muss man zugestehen, dass die »mathematische« Notation einer Formel auch gewisse Vorteile hat. Es ist sprachlich nämlich alles andere als leicht, den Unterschied zwischen $(a \wedge (b \vee c))$ und $((a \wedge b) \vee c)$ auszudrücken (versuchen Sie es doch einmal). Ebenso gibt es in der Umgangssprache fiese Fallstricke: »es gelten nicht a, b und c« bedeutet dasselbe wie »es gelten nicht a, b oder c«. Daher die besagten Antipathien: Mathematiker bevorzugen die symbolbasierte Darstellung, da diese Mehrdeutigkeiten zuverlässig verhindert, Informatiker bevorzugen sie, weil sie maschinenlesbar ist.

Nachdem man die *Syntax* der Aussagenlogik geklärt hat, bleibt die Frage nach der *Semantik* – im konkreten Fall: Wen sollte der Inspektor verhaften? Dazu muss man wissen, welche möglichen »Täterkonstellationen« es aufgrund der Ermittlungsergebnisse geben kann. Prinzipiell gibt es ja acht Möglichkeiten, welche der drei Personen Täter sein könnten, die Ermittlungsergebnisse schließen davon aber viele aus. Wenn genau eine Möglichkeit übrig bleibt, dann können die Haftbefehle rausgehen – schließlich weiß man dann, wer die Täter sind. Wenn mehrere Möglichkeiten übrig bleiben, dann muss weiter ermittelt werden, denn es gilt ja bekanntlich »im Zweifel für den Angeklagten« und Zweifel bestehen in der Tat. Wenn schließlich keine der Möglichkeiten übrig bleiben sollte, dann »kann etwas nicht stimmen«, denn die Ermittlungsergebnisse widersprechen sich gegenseitig.

Wir sind jetzt schon ganz dicht dran an der offiziellen Definition der Semantik der Aussagenlogik. Jedoch sind die Begriffe »Ermittlungsergebnisse«, »prinzipielle Möglichkeiten, wer Täter sein könnte«, »aufgrund der Ermittlungsergebnisse übrig gebliebene Möglichkeiten« und »sich gegenseitig widersprechende Ermittlungsergebnisse« doch etwas lang und unhandlich für einen typischen mathematischen Text: »Satz: Sei φ ein Ermittlungsergebnis, das sich nicht widerspricht. Dann existiert eine Möglichkeit, wer die Täter sein könnten.« ist zwar im wahrsten Sinne des Wortes logisch, aber irgendwie doch etwas umständlich. In Jahrhunderten der Forschung haben sich stattdessen die Begriffe »Formel«, »Welt«, »Modell« und »Kontradiktion« eingebürgert, weshalb der Satz im Lehrbuch heißt »Satz: Sei φ keine Kontradiktion. Dann hat φ ein Modell.« Das gilt dann als wissenschaftlicher, denn es ist kürzer und man versteht es nicht mehr. . .

2.1 Aussagenlogische Formeln

Aussagenlogik – ein Überblick. 2-4

Die *Aussagenlogik* beschäftigt sich mit der *Wahrheit* von *Aussagen*. Sie ist eine der *einfachsten* und *am besten verstandenen Logiken*.
Die Aussagenlogik ist ein *formales System*. Ihre Schlussweisen begegnen uns oft:

- In Gesprächen verwenden wir oft aussagenlogische Argumentationen.
- Schaltkreise in Computern basieren auf Aussagenlogik.
- Die Sicherheit von bestimmten Systemen kann durch Aussagenlogik bewiesen (oder widerlegt) werden.

2.1.1 Aussagen

2-5 **Die Grundlage der Aussagenlogik: Aussagen.**

- Die elementarste Einheit der Aussagenlogik ist die *Aussage*.
- Dieser Begriff ist *umgangssprachlich mehrdeutig*, wir werden ihn deshalb *enger fassen*.
- Schritt 1: Wir lassen als Aussagen nur Sätze oder Satzteile zu, die nur *wahr* oder *falsch* sein können.
- Schritt 2: Wir *abstrahieren* vom Inhalt der Aussagen.

2-6 **Schritt 1: Beispiele und Gegenbeispiele von Aussagen.**

Beispiele: Aussagen

- Lübeck ist eine Stadt.
- $\pi < 4$.
- Die erste Aussage ist falsch.

Beispiele: Keine Aussagen

- Die Farbe gelb ist schön.
- Wir wollen jetzt etwas singen.

✎ Zur Diskussion
Welche der folgenden Sätze sind Aussagen im engeren Sinne?

1. Dieser Satz ist richtig.
2. Gott ist tot.
3. Dieser Satz ist falsch.

2.1.2 Aussagenvariablen

2-7 **Schritt 2: Aussagen und Aussagenvariablen.**

Wir *ignorieren* den *Inhalt* von Aussagen und erlauben nur zwei Aussagen mit *festem* Wahrheitsgehalt: `w` und `f` (Konstante). Für Aussagen mit *unbekanntem oder variablem* Wahrheitsgehalt benutzen wir die *Aussagenvariablen* a, a', a'', a''', …

Beispiel

- Statt »Lübeck ist ein Land« schreiben wir »`f`«.
- Statt »Es regnet« schreiben wir »a«.
- Statt »Gen 5 ist bei schwarzen Schafen vorhanden« schreiben wir »a'«.

2.1.3 Junktoren

2-8 **Aussagen kann man zusammenfügen.**

Mehrere Aussagen lassen sich *zusammenfügen* zu neuen Sätzen mit Wörtern wie beispielsweise »*und*«, »*nicht*« oder »*falls*«. Der Wahrheitsgehalt der entstehenden *Formeln* hängt vom Wahrheitsgehalt der zusammengefügten Aussagen ab. Die zusammenfügenden Wörter nennt man *Junktoren*.

Beispiel

$$\underbrace{\underbrace{\text{Lübeck ist ein Land}}_{\text{Aussage}}\ \underbrace{\textit{und}}_{\text{Junktor}}\ \underbrace{\text{Berlin ist eine Stadt}}_{\text{Aussage}}}_{\text{Formel}}$$

Die grundlegenden Junktoren: Und, Oder, Nicht. 2-9

Drei Junktoren sind besonders wichtig:

Umgangssprache	Logik	alternativ	Java / C	SQL / Lua
»und«	$\wedge$	$\cdot$, weglassen	`&&`	`and`
»oder«	$\vee$	$+$	`||`	`or`
»nicht«	$\neg$	Strich drüber	`!`	`not`

Beispiel

Statt »Er regnet oder es regnet nicht.« schreiben wir »$a \vee \neg a$«.

Fallstricke

Manchmal meint man mit »oder« auch den *Exklusiv-Oder-Junktor*, geschrieben »xor« oder »$\oplus$« . Dies ist besonders bei Sätzen mit »entweder … oder aber … « der Fall. Dieser verhält sich wie der Oder-Junktor, außer wenn beide Aussagen wahr sind; denn dann ist die Formel falsch. Beispiel: »Entweder Lübeck ist eine Stadt, oder aber Berlin ist eine Stadt« entspricht eher »`w` xor `w`«, was falsch ist.

Der Implikations-Junktor. 2-10

Der Implikation-Junktor wird »$\rightarrow$« geschrieben, aber »wenn, dann« gesprochen. Er drückt aus, dass eine Aussage wahr ist, wenn eine andere wahr ist. Es soll also gelten:

- `w` $\rightarrow$ `w` ist eine wahre Formel.
- `w` $\rightarrow$ `f` ist eine falsche Formel.

- Statt »Wenn $4 > \pi$ gilt, dann gilt $5 > \pi$« schreiben wir `w` $\rightarrow$ `w`, was wahr ist.
- Statt »Wenn $4 > \pi$ gilt, dann gilt $3 > \pi$« schreiben wir `w` $\rightarrow$ `f`, was falsch ist.

Was passiert, wenn die Aussage, aus der etwas folgen soll (auch *Prämisse* genannt), schon falsch ist?

- Beispiel: »Wenn $2 > \pi$ gilt, dann gilt $4 > \pi$.«
- Beispiel: »Wenn $2 > \pi$ gilt, dann gilt $3 > \pi$.«

Wir *definieren* später:

- `f` $\rightarrow$ `w` ist eine wahre Formel (!).
- `f` $\rightarrow$ `f` ist eine wahre Formel (!).

Der Äquivalenz-Junktor. 2-11

Der Äquivalenz-Junktor wird »$\leftrightarrow$« geschrieben, aber »genau dann, wenn« gesprochen. Er drückt aus, dass eine Aussage genau dann wahr ist, wenn eine andere wahr ist. Also:

- `w` $\leftrightarrow$ `w` ist eine wahre Formel.
- `f` $\leftrightarrow$ `w` ist eine falsche Formel.
- `w` $\leftrightarrow$ `f` ist eine falsche Formel.
- `f` $\leftrightarrow$ `f` ist eine wahre Formel.

✎ Zur Übung 2-12

Zur Ihrer nächsten Party habe Sie drei besondere Freunde eingeladen: Alice, Bob und Charly. Die Variablen a, b und c stehen nun für die Aussagen »Alice kommt«, »Bob kommt« und »Charly kommt«.
Leider ist nicht ganz klar, wer nun kommen wird, denn:

1. Alice und Bob kommen oder Bob und Charly kommen, aber nicht beides.
2. Keiner von Alice, Bob und Charly kommt.
3. Keiner von Alice, Bob oder Charly kommt.

Formulieren Sie jeden der Sätze einzeln als Formeln sowie als Java-Ausdrücke.

2.1.4 Formeln und ihre Syntax

2-13

Die Syntax der Aussagenlogik.

Die *Syntax der Aussagenlogik* beschreibt, welche *Zeichenketten (Strings)* nun *erlaubte Formeln* sind. Wie immer sagt sie nichts über die Bedeutung dieser Formeln.

▶ Definition

Die Menge $L_{\text{Aussagenlogik}}$ der *Formeln der Aussagenlogik* ist die kleinste Menge aller Unicode-Strings mit folgenden Eigenschaften:

1. Die Ein-Zeichen-Strings `f`" und "`w`" sind Elemente von $L_{\text{Aussagenlogik}}$.
2. Strings der Form "$a'^{\cdots'}$" sind Elemente von $L_{\text{Aussagenlogik}}$, wobei auch ein einzelnes a erlaubt ist.
3. Ist der String φ ein Element von $L_{\text{Aussagenlogik}}$, so auch der um ein Zeichen längere String $\neg\varphi$.
4. Sind φ und ψ Elemente von $L_{\text{Aussagenlogik}}$, so auch die Strings $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ und $(\varphi \leftrightarrow \psi)$.

Skript

Die obige Definition der Menge $L_{\text{Aussagenlogik}}$ ist ein wenig »ad hoc« – in der (Theoretischen) Informatik wird die Syntax von (logischen oder Programmier-)Sprachen normalerweise mit Hilfe von *Grammatiken* beschrieben. Im Folgenden findet sich für alle Interessierte eine solche Beschreibung; Grammatiken sind aber nicht Teil dieser Veranstaltung.

▶ Definition: Syntax der Aussagenlogik im Sinne der Theoretischen Informatik

Die *Syntax der Aussagenlogik* eine *Sprache* $L_{\text{Aussagenlogik}}$, die alle *Formeln der Aussagenlogik* enthält. Das *Alphabet* dieser Sprache ist:

$$\Sigma_{\text{Aussagenlogik}} = \{\mathtt{f}, \mathtt{w}, a, {}', (,), \wedge, \vee, \to, \leftrightarrow, \neg\}.$$

Die Sprache wird erzeugt von der folgenden Grammatik:

1. Die *Terminale* sind gerade das Alphabet $\Sigma_{\text{Aussagenlogik}}$.
2. Die *Nonterminale* sind die Symbole F (für »Formel«), A (für »atomare Formel«) und V (für »Variable«).
3. Das *Startsymbol* ist F.
4. Die Regeln sind:

$$F \to A \mid (F \wedge F) \mid (F \vee F) \mid \neg F \mid (F \to F) \mid (F \leftrightarrow F)$$
$$A \to \mathtt{f} \mid \mathtt{w} \mid V$$
$$V \to a \mid V'$$

2-14

Einige Vereinfachungen beim Schreiben.

- Statt a'''''''' werden wir auch Buchstaben wie p oder q oder b verwenden oder auch p_1 oder p_2.
- Äußere Klammern lassen wir auch gerne weg.
- Später werden wir noch mehr Klammern weglassen.
- Statt `w` schreibt man auch `true` oder `t` oder `1` oder $\top$.
- Statt `f` schreibt man auch `false` oder `0` oder $\bot$.

2.2 Semantik der Aussagenlogik

2.2.1 Welten

Das Problem: Wie legen wir eine Semantik fest? 2-15

Bei der *Semantik* geht es darum, einem *syntaktisch korrekten Wort* eine *Bedeutung* zuzuweisen. In unserem Fall sind syntaktische korrekte Wörter *Formeln*. Wir müssen also für Formeln festlegen, ob diese *wahr* oder *falsch* sind. Beispielsweise werden wir gleich festlegen, dass die Formel $(\mathtt{w} \land \neg \mathtt{f})$ eine *wahre Formel* ist. Bei Formeln mit Variablen ist es nicht immer möglich, einen Wahrheitsgehalt zuzuordnen. Beispiel: Den Satz »Es regnet oder die Tür ist nicht auf« könnte man formalisieren als $(r \lor \neg t)$. Ist dieser Satz nun wahr oder falsch?

Die Lösung: Das Konzept der Welten. 2-16

Alle Probleme mit dem Wahrheitsgehalt von Formeln *verschwinden*, wenn man den Wahrheitsgehalt *aller Variablen* kennt. Wenn man den Wahrheitsgehalt aller Variablen festlegt, entsteht eine *Welt*. Eine Formel kann in der einen Welt wahr sein, in einer anderen falsch sein.

Zwei Welten und die Belegung der Variablen in diesen Welten. 2-17

Es steht h für »hat Wasser«, l für »besitzt Leben« und s für »ist Sonnenplanet«.

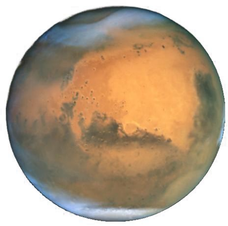
Welt 1 (die Erde)

- ist wasserreich (h ist wahr)
- hat Leben (l ist wahr)
- kreist um Sonne (s ist wahr)

NASA image, public domain

Welt 2 (der Mars)

- ist wasserarm (h ist falsch)
- hat kein Leben (l ist falsch)
- kreist um Sonne (s ist wahr)



NASA image, public domain

2.2.2 Variablenbelegungen

Das Konzept der Variablenbelegung. 2-18

Welten unterscheiden sich dadurch, welche Variablen in ihnen wahr sind, also wie die Variablen *belegt* sind.

▶ Definition

$V_{\text{Aussagenlogik}}$ bezeichne die Menge der aussagenlogischen Variablen $\{a, a', a'', a''', \dots\}$, wobei wir für diese im Folgenden auch andere Symbole wie $x, y, z, \dots$ verwenden werden.

▶ Definition

Eine *Variablenbelegung* ist eine Funktion $\beta\colon V \to \{0,1\}$, die auf einer Teilmenge $V \subseteq V_{\text{Aussagenlogik}}$ definiert ist.

Die Wahrheitswerte von Variablen, die nicht zu V gehören, interessieren uns zunächst nicht.

Merke

In der Aussagenlogik gilt: *Welt* = *Variablenbelegung*

2.2.3 Auswertungen

2-19 **Die Auswertung einer Formel.**

Hat man eine aussagenlogische Formel gegeben und eine Welt (also eine Variablenbelegung), so ist der Wahrheitsgehalt der Formel *festgelegt*. Man kann den Wahrheitswert einer Formel nun *auswerten*, ganz ähnlich wie man den Wert einer *arithmetischen Formel* berechnet: $2+(3+1)=6$ – beide Seiten repräsentieren dieselbe natürliche Zahl. Dazu berechnet man schrittweise die Wahrheitswerte der *Teilformeln*, bis man beim Wert der ganzen Formel angelangt ist (wie einfach: wir »rechnen« nicht über $\mathbb{N}$ sondern nur über $\{0,1\}$). Beispiel: Gilt in einer Welt, dass x wahr ist und y falsch, dann gilt:

$$\underbrace{(\underbrace{\neg\underbrace{(x \lor y)}_{\text{wahr}}}_{\text{falsch}} \land x)}_{\text{falsch}}.$$

2-20 **Zulässige Variablenbelegungen.**

Damit eine Auswertung Sinn macht, muss natürlich jeder Variable einer Formel auch durch die Variablenbelegung etwas zugeordnet werden.

▶ **Definition:** Zulässige Variablenbelegung

Eine Variablenbelegung $\beta\colon V \to \{0,1\}$ heißt *zulässig* für eine Formel φ, wenn alle in φ vorkommenden Variablen in V enthalten sind.

Beispiel

Die Variablenbelegung $\beta\colon \{x,y\} \to \{0,1\}$ mit $\beta(x)=1$ und $\beta(y)=0$ ist zulässig für $(x \lor y) \to x$ und für $x \lor x \lor x$, aber nicht zulässig fürr z oder $x \to z$.

Beispiel

Eine Variablenbelegung $\beta\colon V_{\text{Aussagenlogik}} \to \{0,1\}$, die einfach jeder Variable aus der Menge $V_{\text{Aussagenlogik}}$ etwas zuordnet, ist für jede Formel zulässig.

2-21 **Definition der Auswertungsfunktion.**

▶ **Definition:** Auswertungsfunktion

Sei $\beta\colon V \to \{0,1\}$ eine Variablenbelegung und sei L die Teilmenge von $L_{\text{Aussagenlogik}}$ der für β zulässigen Formeln. Die *Fortsetzung* $\hat\beta\colon L \to \{0,1\}$ weist jeder Formel $\varphi \in L$ einen Wert $\hat\beta(\varphi)$ zu, der sich induktiv gemäß ihrem Aufbau wie folgt berechnet:

φ	$\hat\beta(\varphi)$
x	$\beta(x)$
$\mathtt{w}$	1
$\mathtt{f}$	0
$\neg\psi$	$1-\hat\beta(\psi)$
$(\psi \land \rho)$	$\min\{\hat\beta(\psi), \hat\beta(\rho)\}$
$(\psi \lor \rho)$	$\max\{\hat\beta(\psi), \hat\beta(\rho)\}$
$(\psi \to \rho)$	$0,\ \text{falls } \hat\beta(\psi)=1 \text{ und } \hat\beta(\rho)=0,\ \text{andernfalls } 1$
$(\psi \leftrightarrow \rho)$	$0,\ \text{falls } \hat\beta(\psi) \neq \hat\beta(\rho),\ \text{andernfalls } 1$

Skript

Es fällt einem zunächst nicht auf, aber es ist gar nicht klar, ob diese Definition überhaupt »korrekt« ist. Normalerweise denkt man ja, dass Definitionen gar nicht »falsch« sein können, denn definieren kann man scheinbar beliebige Dinge. Jedoch darf eine Definition nicht in sich widersprüchlich sein: Beispielsweise könnte man nicht definieren »sei f eine Funktion mit $f(2-2)=5$ und $f(1-1)=9$,« da nun reichlich unklar wäre, ob $f(0)$ nun 5 oder doch eher 9 ist. Im Fall der obigen Definition der Auswertungsfunktion könnte etwas ähnliches passieren: Gibt es vielleicht Formeln φ, die auf verschiedene Arten »geparst« werden können und für die Definition unterschiedliche Wahrheitswerte festlegt? Dass dies *nicht* passieren kann, besagt folgendes Lemma:

▶ **Lemma:** Parsing-Lemma

Sei $\varphi \in L_{\text{Aussagenlogik}}$. Dann ist φ von genau einer der folgenden Bauarten:

- *φ ist eine atomare Formel, also $\varphi = \mathtt{w}$ oder $\varphi = \mathtt{f}$ oder $\varphi = a^{\prime\prime\prime\cdots\prime}$.*

- *φ ist von der Form $\neg\psi$, wobei $\psi \in L_{\text{Aussagenlogik}}$.*
- *φ ist von der Form $(\psi \circ \rho)$, wobei $\psi, \rho \in L_{\text{Aussagenlogik}}$ eindeutig sind und $\circ$ einer der Junktoren $\wedge$, $\vee$, $\to$ oder $\leftrightarrow$ ist.*

Achtung: Das Lemma würde *nicht* gelten, wenn die Syntax der Aussagenlogik leicht ändern würde; zum Beispiel, indem man die Klammern wegließe.

Kommentare zum Beweis

Beweis. Wir beweisen die Behauptung durch eine Induktion über die Länge von φ. Für die Länge 0 ist die Behauptung trivialerweise wahr, da es gar keine Formel der Länge 0 gibt. Für die Länge 1 ist die Behauptung ebenfalls wahr, da es als ableitbare Zeichenketten der Länge 1 nur `w`, `f` und a gibt.
Für den Induktionsschritt sei nun ein φ der Länge $n+1 \geq 2$ gegeben und die Behauptung sei schon für alle φ der Länge kleiner oder gleich n gezeigt. Da $\varphi \in L_{\text{Aussagenlogik}}$ gilt, muss es eine Ableitung von φ geben. Im ersten Schritt dieser Ableitung muss eine Regel der Form $F \to \dots$ angewandt worden sein. Wir unterscheiden nun verschiedene Fälle, je nachdem, welche Regel dies war:

$F \to A$ Da φ Länge mindestens 2 hat, kann der nächste Ableitungsschritt nur $A \Rightarrow V$ gewesen sein. Dann muss aber genau n mal der Schritt $V \Rightarrow V'$ angewandt worden sein und schließlich $V \Rightarrow a$, da φ ja Länge $n+1$ hat. Dann muss φ die Form $a'''^{\cdots}{}'$ gehabt haben, wie behauptet.

$F \to \neg F$ In diesem Fall muss φ mit dem Zeichen $\neg$ beginnen. Nennen wir den Rest ψ, so gilt $F \Rightarrow^* \psi$ und somit $\psi \in L_{\text{Aussagenlogik}}$.

$F \to (F \circ F)$ Hierbei ist $\circ$ ein beliebiger Junktor. Dann muss φ von der Bauart $(\psi \circ \rho)$ sein und weiterhin müssen $F \Rightarrow^* \psi$ und auch $F \Rightarrow^* \rho$ gelten. Somit gilt $\psi, \rho \in L_{\text{Aussagenlogik}}$.

Es bleibt zu zeigen, dass bei der letzten Möglichkeit ψ und ρ eindeutig sind. Mit anderen Worten, wir müssen zeigen, dass sich φ nicht etwa auf verschiedene Arten zerlegen lässt. Wäre dies der Fall, so müsste es ψ' und ρ' geben mit $\psi \circ \rho = \psi' \circ \rho'$ und ψ müsste ein echter Präfix (ein Anfangsstück) von ψ' sein oder umgekehrt. Nehmen wir ohne Beschränkung der Allgemeinheit an,[1] das erstere sei der Fall. Dann muss ψ' den Junktor $\circ$ enthalten und folglich mit einer Klammer anfangen. Daraus folgt wiederum, dass auch ψ mit einer Klammer anfangen muss.
Wir behaupten nun zwei Dinge: (1) Die Anzahl der öffnenden und schließenden Klammern ist in jedem Wort von $L_{\text{Aussagenlogik}}$ gleich, was man ganz leicht durch Induktion über die Ableitungslänge der Wörter zeigt.[2] (2) Für alle $w \in L_{\text{Aussagenlogik}}$, die mit einer Klammer anfangen, gilt, dass in jedem nichtleeren echten Präfix von w ist die Anzahl der öffnenden Klammern größer als die Anzahl der schließenden Klammern. Auch dies sieht man leicht durch Induktion. Daraus folgt aber, dass ψ wegen (1) eine ausgeglichene Anzahl von Klammern haben muss und wegen (2) dies doch nicht Fall ist. Dies ist ein Widerspruch und folglich kann die alternative Zerlegung von φ doch nicht existieren. □

[1] Sehen Sie, warum man das annehmen darf?

[2] »Was man leicht zeigt« bedeutet »weder ich noch der Leser haben Lust, das jetzt wirklich zu zeigen«.

✎ Zur Übung

2-22

Sei $\beta(x) = 1$, $\beta(y) = 0$ und $\beta(z) = 0$. Wie lautet $\hat{\beta}(\varphi)$ für folgende φ?

1. $(x \wedge y)$
2. $((x \to x) \to z)$
3. y
4. $(x \wedge y \wedge z)$
5. $z \to (x \wedge ((\neg\neg\neg(z \leftrightarrow x) \vee y \leftrightarrow (x \wedge \neg x)))$

2.3 Semantische Begriffe

2.3.1 Modelle

2-23 **In welcher Welt gilt eine Formel?**
Sei φ die Formel $(l \wedge s)$ und β die Welt »Erde« (). Die Formel besagt »Auf der Welt gibt es Leben und sie gehört zum Sonnensystem«. Sie *gilt* in der Welt β, da $\hat{\beta}(\varphi) = 1$. Deshalb werden wir β ein *Modell von* φ nennen. Die Formel *gilt nicht* in der Welt des Mars, da sie dort zu 0 auswertet. Entsprechend ist β *kein Modell von* φ.

▶ **Definition:** Modell
Sei φ eine Formel und β eine für φ zulässige Variablenbelegung. Falls $\hat{\beta}(\varphi) = 1$, so nennen wir β *ein Modell für* φ. Schreibweise:

$$\beta \models \varphi.$$

✎ **Zur Diskussion**
Wie viele Modelle hat $(x \vee y)$?

2-24 **Kleine Erweiterung: Modelle von Formelmengen**

▶ **Definition:** Modelle von Formelmengen
Sei $\beta: V \to \{0,1\}$ eine Variablenbelegung und Φ eine Menge von für β zulässigen Formeln (also $\Phi \subseteq L_{\text{Aussagenlogik}}$ und in jedem $\varphi \in \Phi$ kommen nur Variablen aus V vor). Wir schreiben

$$\beta \models \Phi,$$

und sagen β *ist ein Modell von* Φ, falls $\beta \models \varphi$ für alle $\varphi \in \Phi$ gilt.

Merke
Ein Modell für eine Formelmenge ist eine Welt, die *alle* Formeln in der Menge wahr macht.

2.3.2 Erfüllbarkeit

2-25 **Der Erfüllbarkeitsbegriff.**
Modelle sind wichtig, da sie uns die Umstände aufzeigen, unter denen eine Formel wahr wird. Eine erste Frage ist, ob eine Formel *überhaupt wahr werden kann*, ob sie also *überhaupt ein Modell besitzt*. So ist $(l \wedge \neg l)$, also »die Welt besitzt Lebewesen und sie hat kein Leben«, weder für die Erde noch für den Mars noch für Vulkan noch für sonst irgendeine Welt wahr.

▶ **Definition**
Eine Formel φ heißt *erfüllbar*, wenn sie ein Modell hat. (Wenn es also eine Variablenbelegung gibt, so dass die Formel wahr wird.) Schreibweise (erfüllbar = *sat*isfiable im Englischen):

$$\varphi \in \textsc{sat}.$$

2.3.3 Tautologien

2-26 **Der Tautologiebegriff.**
Eine *Tautologie* ist eine Formel, die »immer wahr ist«. Zum Vergleich: eine *erfüllbare Formel* muss nur *ein Modell* haben, bei einer *Tautologie* muss *jede Welt ein Modell sein*. Eine typische Tautologie ist »es gibt Wasser genau dann, wenn es Wasser gibt«, sie ist aber nicht sehr interessant.

▶ **Definition**
Eine Formel φ ist eine *Tautologie*, wenn jede zulässige Welt ein Modell der Formel ist (wenn sie also unter jeder zulässigen Variablenbelegung β wahr ist.) Schreibweise:

$$\models \varphi \quad \textit{oder} \quad \varphi \in \textsc{taut}$$

als Abkürzung für: *für alle* β *gilt* $\beta \models \varphi$.

2.3.4 Kontradiktionen

Der Kontradiktionsbegriff. 2-27

Eine *Kontradiktion* ist das »Gegenteil« einer Tautologie: sie ist »immer falsch«. Sie darf also *kein Modell* haben. Tatsächlich ist die Kontradiktion somit *eher das Gegenteil einer erfüllbaren Formel*.

▶ Definition

Eine Formel φ ist eine *Kontradiktion*, wenn sie kein Modell hat (wenn sie also unter jeder Variablenbelegung falsch ist).

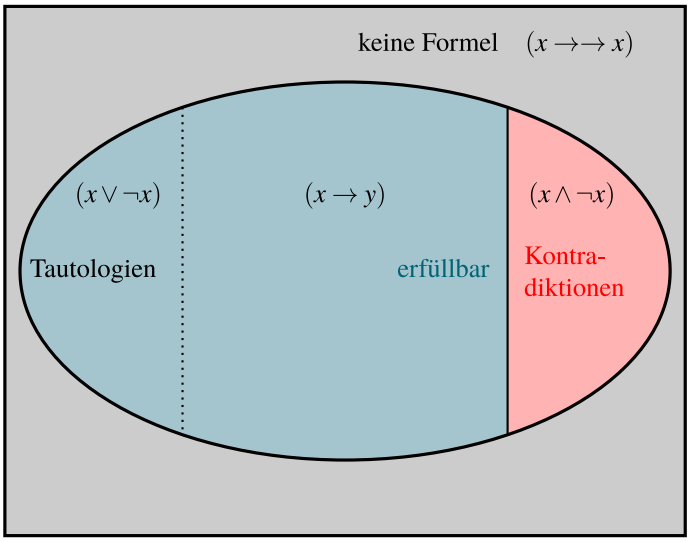
✎ Zur Übung 2-28

Geben Sie zu jeder der folgenden Formeln an, ob diese erfüllbar sind, ob sie Kontradiktionen sind und/oder Tautologien.

1. $(x \wedge \neg y)$
2. $(z \vee \neg z)$
3. $(\mathtt{w} \wedge \mathtt{f})$
4. $(\mathtt{w} \wedge \mathtt{w})$
5. $(x \leftrightarrow \mathtt{f})$

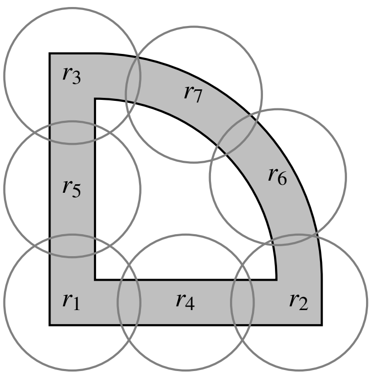
Lage der Formelmengen zueinander. 2-29

Alle Strings



2.3.5 Eine kleine Anwendung

Beispielanwendung: Aufstellung von WLAN-Routern 2-30



Im Informatikgebäude soll der WLAN-Empfang verbessert werden, indem mehr Router aufgestellt werden. Router, die nahe beieinander sind, müssen auf unterschiedlichen Frequenzen funken, vereinfachend gibt es nur zwei Frequenzen. Die Variable r_i möge wahr sein, wenn r_i auf der ersten Frequenz funkt. Wir suchen also ein Modell der Formelmenge

$$\{r_1 \leftrightarrow \neg r_4, r_4 \leftrightarrow \neg r_2, r_2 \leftrightarrow \neg r_6, r_6 \leftrightarrow \neg r_7, r_7 \leftrightarrow \neg r_3,\\ r_3 \leftrightarrow \neg r_5, r_5 \leftrightarrow \neg r_1\}.$$

Zusammenfassung dieses Kapitels

2-31

▶ Syntaktischer Aufbau von Formeln

Aussagenlogische Formeln sind *Strings* (= Wörter im Sinne der Theoretischen Informatik) einer der folgenden *rekursiv definierten* Formen:

- Die Konstanten `w` und `f`.
- Das Symbol a, gefolgt von beliebig vielen Strich-Symbolen. (Diese Wörter nenne wir dann *Variablen*.)
- Das Symbol $\neg$ gefolgt von einer Formel.
- Zwei Formeln, die durch einen der Junktoren $\wedge$, $\vee$, $\rightarrow$ oder $\leftrightarrow$ verbunden sind und durch runde Klammern umschlossen sind.

▶ Semantische Grundbegriffe der Aussagenlogik

Variablenbelegung Eine Fuktion $\beta\colon V \to \{0,1\}$.

Welt Anderes Wort für Variablenbelegung.

Auswertungsfunktion Die Funktion $\hat\beta$ »setzt β« fort, indem sie allen Formeln einen Wahrheitswert zuweist (β macht dies nur für Variablen).

Modell einer Formel φ Ein Welt β mit $\hat\beta(\varphi) = 1$.

Erfüllbare Formel Formel, die ein Modell hat.

Kontradiktion Formel, die kein Modell hat.

Tautologie Formel, für die jede Welt ein Modell ist.

Übungen zu diesem Kapitel

Übung 2.1 Umgangssprachliche Aussagen formalisieren, mittel

Herakles heroische Heldentaten, 1. Orakelspruch

Schon kurz nach der Geburt der Zwillingsbrüder Herakles und Eurystheus entstand ein Streit, wer von beiden der rechtmäßige Herrscher sei. Dazu wurden die drei bekanntesten Orakel befragt.

Das Ammonion gab bekannt, dass die Orakelsprüche aus Klaros grundsätzlich falsch seien. Ebenso ließ das Orakel aus Klaros verlauten, dass die Orakelsprüche aus Delphi samt und sonders unzutreffend seien. Das Orakel aus Delphi jedoch behauptete, sowohl die Sprüche des Ammonions als auch die des Orakels in Klaros seien unwahr.

Wem sollten die armen Griechen nun glauben? Führen Sie zunächst drei Variablen x_A, x_K und x_D mit folgenden Interpretationen ein:

- x_A: »Das Ammonion sagt die Wahrheit.«
- x_K: »Das Orakel von Klaros sagt die Wahrheit.«
- x_D: »Das Orakel von Delphi sagt die Wahrheit.«

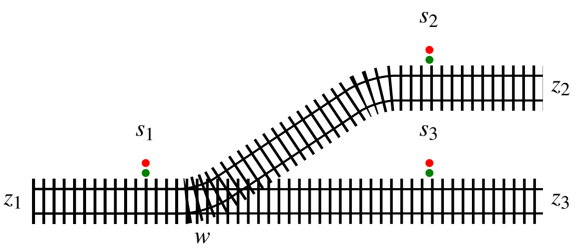
Formalisieren Sie anschließend Ihr Wissen über die Orakel als aussagenlogische Formeln. Aus dem Spruch des Ammonions kann man beispielsweise »$a \leftrightarrow \neg b$« ableiten, d. h. das Ammonion sagt die Wahrheit genau dann, wenn das Orakel aus Klaros tatsächlich lügt.

Durch diese Formalisierung ist das Problem natürlich noch nicht gelöst (dazu brauchen wir die Semantik aus dem nächsten Kapitel), aber Sie fühlen sich jetzt sicherlich schon viel besser.

(Diese Aufgabe ist dem Buch *Logik für Informatiker* von Martin Kreuzer und Stefan Kühling entnommen.)

Übung 2.2 Sicherheitsanforderungen formalisieren, mittel

Eine Weiche an einer Bahnanlage ist wie folgt aufgebaut:



Die Variable w gibt die Stellung der Weiche an (»Abbiegen« oder »Geradeaus«). Die Variablen z_1 bis z_3 geben an, ob ein Zug in dem entsprechenden Abschnitt ist. Die Signale s_1 bis s_3 geben an, ob ein Zug von außen Richtung Weiche fahren darf.

Formulieren Sie nun Anforderungen an das System zunächst umgangssprachlich und dann als Formeln. Überlegen Sie, wie Sie sicherstellen können, alle Anforderungen abgedeckt zu haben.

Übung 2.3 Semantische Eigenschaften von Formeln, leicht

Bestimmen Sie für jede der folgenden Formeln, ob sie erfüllbar oder eine Tautologie oder eine Kontradiktion ist. Geben Sie für Formeln, die weder eine Tautologie noch eine Kontradiktion sind, eine Variablenbelegung an, die ein Modell ist, und eine Variablenbelegung, die kein Modell ist.

1. $(x \wedge z) \vee y$
2. $(x \vee \neg x) \leftrightarrow \mathtt{w}$
3. $(\mathtt{w} \wedge \neg(x \rightarrow y))$
4. $((y \vee x) \wedge z) \leftrightarrow (x \wedge z)$
5. $(x \rightarrow b) \leftrightarrow (\neg b \rightarrow \neg x)$
6. $(\neg(x \vee y)) \rightarrow \neg y$
7. $(\neg x \vee b) \wedge (x \rightarrow b)$
8. $((x \wedge b) \rightarrow c) \wedge \neg b$
9. $((x \rightarrow y) \rightarrow z) \rightarrow (x \rightarrow z)$
10. $(\neg b \rightarrow \neg x) \leftrightarrow (\neg x \wedge b)$
11. $(x \rightarrow (y \rightarrow z)) \rightarrow (x \rightarrow z)$

Übung 2.4 Formeln auswerten, leicht

Gegeben ist eine Variablenbelegung $\beta\colon \{x_1, x_2, x_3, x_4\} \rightarrow \{0, 1\}$ mit $\beta(x_1) = 1$, $\beta(x_2) = 0$, $\beta(x_3) = 0$ und $\beta(x_4) = 1$. Geben Sie für alle Teilformeln der folgenden Formeln den Wahrheitswert unter $\hat{\beta}$ an.

1. $((x_4 \rightarrow x_2) \wedge (x_1 \rightarrow \neg x_2)) \vee (\neg x_2 \wedge x_3)$
2. $((((\neg x_1 \vee x_2) \rightarrow x_1) \vee x_3) \leftrightarrow x_1) \vee (x_1 \wedge x_4)$

Übung 2.5 Formel mit einer bestimmten Anzahl von Modellen finden, mittel

Wir definieren die Menge $V_n = \{a_1, \ldots, a_n\}$ als die Variablenmenge mit n aussagenlogischen Variablen und betrachten Belegungen $\beta\colon V_n \rightarrow \{0, 1\}$. In diesem Fall ist $V_n \subseteq V_{\text{Aussagenlogik}}$ endlich und es gibt genau 2^n unterschiedliche Belegungen.

Geben Sie für $n = 4$ eine Formel φ an, die genau vier Modelle $\beta\colon V_n \rightarrow \{0, 1\}$ hat. Das heißt, es soll nur vier unterschiedliche Belegungen β geben, so dass $\hat{\beta}(\varphi) = 1$.

Übung 2.6 Formel mit einer bestimmten Anzahl von Modellen finden, mittel

Beschreiben Sie, wie man allgemein für jedes n eine Formel mit Variablen in V_n konstruieren kann, die genau n Modelle hat.

Übung 2.7 Umgangssprachliche Aussagen lösen, mittel

In Übung 2.1 wurde bereits ein Text mittels der Aussagenlogik formalisiert. Lösen Sie nun die Aufgabe, indem Sie ein Modell für alle Aussagen angeben.

Übung 2.8 Umgangssprachliche Aussagen lösen, mittel

Unendliche Weiten, Episode 1: Die Lügen der Polits

Die Enterprise fliegt zu Forschungszwecken zum weitgehend unbekannten Planeten Warlüg. Man weiß bisher nur, dass sich das Volk in drei Stämme unterteilt, die Xurs, welche immer die Wahrheit sagen, die Polits, notorische Lügner, und die Yzys, die lügen oder die Wahrheit sagen, je nach Lust und Laune. Captain Archer und Sub-Commander T'Pol beamen sich auf den Planeten und begegnen drei Einheimischen. Dem äußeren Erscheinungsbild nach zu urteilen ist jeder der drei Stämme vertreten.

Archer: *»Von welchem Stamm seid ihr?«*

Der erste sagt: *»Der dritte ist ein Polit.«*

Der zweite sagt: *»Der erste ist ein Xur.«*

Der dritte sagt: *»Ich bin ein Yzy.«*

Archer zu T'Pol: *»So kommen wir nicht weiter.«*

T'Pol blickt Archer verständnislos an: »Aber es ist doch offensichtlich, wer von welchem Stamm ist. …«

Nämlich?

(Diese Aufgabe ist dem Buch *Logik für Informatiker* von Martin Kreuzer und Stefan Kühling entnommen.)

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

Prüfungsfrage 2.9

12 min → Lösung

Umgangsprachliche Aussagen formalisieren

Von dem Wolf, dem Bären und dem Hamster

Vor dem letzten Geburtstag des Bären planten der Hamster und der Wolf einen Kuchen für den Bären zu backen. Über das Rezept gerieten Sie jedoch in Streit.

Der Wolf sagte: »Wenn Eier in den Kuchen kommen, dann isst der Bär nichts von dem Kuchen!«

Der Hamster widersprach: »Fehlen die Eier, dann kann man keinen Apfelkuchen backen! Und der Bär isst genau dann Kuchen, wenn es Apfelkuchen gibt.«

»Aber der Bär muss von dem Kuchen essen!« entgegnete der Wolf.

Formalisieren Sie die Aussagen des Hamsters und des Wolfs durch eine aussagenlogische Formel. (Die Formel reicht aus; sie sollen nicht überprüfen, ob die Formel erfüllbar oder kontradiktorisch ist.) Geben Sie dabei explizit an, wofür Ihre Variablen stehen und was gilt, falls sie mit 0 oder 1 belegt werden.

Nach dem Lösen dieser Aufgabe geht die Geschichte wie folgt weiter:

Der clevere Hamster hatte im vergangenen Jahr bereits die Vorlesung »Logik für Informatiker« besucht und die Übungen 4.6 und 6.6 gelöst. Mit diesem Wissen blieb dem Hamster nichts anderes übrig als zu rufen: »Das geht doch gar nicht!« – »Wir müssen das aber hinbekommen!« brüllte der störrische Wolf. Der Wolf verbat dem Hamster darauf das Durchqueren seines Waldes und versuchte erfolglos den Kuchen zu backen.

Prüfungsfrage 2.10

12 min → Lösung

Umgangsprachliche Aussagen formalisieren

Bieter Dohlen in »DSDS-CS«

Bieter Dohlen, Tina Gurnal und Durl Götek sind die Juroren der neuen TCS-Casting-Show DSDS-CS. In dieser Sendung wird der nächste Informatik-Superstar gesucht.

Im Recall haben sich viele Studierende vorgestellt. Nun beraten die Juroren, wer in die nächste Runde kommt.

Bieter Dohlen beginnt: »Wenn Edsger weiterkommt, dann muss auch Alan in die nächste Runde! Und ich bin der Meinung, dass Dern ausscheiden sollte.«

Tina sagt: »Edsger oder Dern müssen rausfliegen!«

Abschließend meint Juror Götek: »Sollte Dern weiterkommen, dann kommt auch Alan weiter. Sowieso kommt Alan genau dann weiter, wenn auch Edsger die nächste Runder erreicht.«

Formalisieren Sie die Aussagen der Juroren durch eine aussagenlogische Formel. (Die Formel reicht aus; sie sollen nicht überprüfen, ob die Formel erfüllbar oder kontradiktorisch ist.) Geben Sie dabei explizit an, wofür Ihre Variablen stehen und was gilt, falls sie mit 0 oder 1 belegt werden.

Prüfungsfrage 2.11

18 min → Lösung

Semantische Eigenschaften von aussagenlogischen Formeln

Bestimmen Sie für jede der folgenden Formeln, ob sie erfüllbar oder eine Tautologie oder eine Kontradiktion ist. Geben Sie für Formeln, die weder eine Tautologie noch eine Kontradiktion sind, eine Variablenbelegung an, die ein Modell ist, und eine Variablenbelegung, die kein Modell ist.

1. $(x \to z) \wedge y$
2. $(\neg x \to \neg b) \leftrightarrow (b \to x)$
3. $((x \to y) \to z) \wedge \neg(x \vee z)$

Prüfungsfrage 2.12

18 min → Lösung

Wie Prüfungsfrage 2.11, aber für:

1. $(p \wedge q) \vee (\neg p \wedge \neg q)$
2. $p \to (q \to r)$
3. $(p \vee \neg p) \wedge (q \vee \neg q) \wedge (r \vee \neg r)$

Prüfungsfrage 2.13

18 min → Lösung

Wie Prüfungsfrage 2.11, aber für:

1. $(\mathtt{w} \vee x) \to (y \wedge \neg y)$
2. $\big(x \leftrightarrow (b \vee c)\big) \wedge \big(\neg x \to (b \wedge c)\big)$
3. $\big((\neg x \vee b) \vee (b \wedge c)\big) \to \mathtt{f}$

Lösung zu 2.9

Wir definieren folgende Variablen:

- e Eier kommen in den Kuchen genau dann, wenn $\beta(e) = 1$.
- b Der Bär isst vom Kuchen genau dann, wenn $\beta(b) = 1$.
- a Es gibt Apfelkuchen, genau dann wenn $\beta(a) = 1$.

1. »Wenn Eier in den Kuchen kommen, dann isst der Bär nichts von dem Kuchen!«
   $e \to \neg b$
2. »Fehlen die Eier, kann man keinen Apfelkuchen backen!«
   $\neg e \to \neg a$
3. »Und der Bär isst genau dann Kuchen, wenn es Apfelkuchen gibt.«
   $b \leftrightarrow a$
4. »Aber der Bär muss von dem Kuchen essen!«
   b

Die gesuchte Formel ist somit $(e \to \neg b) \wedge (\neg e \to \neg a) \wedge (b \leftrightarrow a) \wedge b$.

Lösung zu 2.10

Wir definieren die folgenden Variablen:

- e Edsger kommt eine Runde weiter genau dann, wenn $\beta(e) = 1$.
- a Alan kommt eine Runde weiter genau dann, wenn $\beta(b) = 1$.
- d Dern kommt eine Runde weiter genau dann, wenn $\beta(a) = 1$.

1. »Wenn Edsger weiterkommt, dann muss auch Alan in die nächste Runde!«
   $e \to a$
2. »Und ich bin der Meinung, dass Dern ausscheiden sollte.«
   $\neg d$
3. »Edsger oder Dern müssen rausfliegen!«
   $\neg e \vee \neg d$
4. »Sollte Dern weiterkommen, dann kommt auch Alan weiter.«
   $d \to a$
5. »Sowieso kommt Alan genau dann weiter, wenn auch Edsger die nächste Runder erreicht.«
   $a \leftrightarrow e$

Die gesuchte Formel ist somit

$$(e \to a) \wedge (\neg d) \wedge (\neg e \vee \neg d) \wedge (d \to a) \wedge (a \leftrightarrow e).$$

Lösung zu 2.11

1. Die Formel $(a \to a'') \land a'$ ist weder eine Tautologie noch eine Kontradiktion. Ein Modell ist die Belegung, die alle Variablen auf 1 setzt; kein Modell ist die Belegung, die alle Variablen auf 0 setzt.
2. Die Formel $(\neg a \to \neg b) \leftrightarrow (b \to a)$ ist ein Tautologie.
3. Die Formel $((a \to a') \to a'') \land \neg(a \lor a'')$ ist eine Kontradiktion.

Lösung zu 2.12

1. Die Formel $(p \land q) \lor (\neg p \land \neg q)$ ist weder eine Tautologie noch eine Kontradiktion. Ein Modell ist die Belegung $\beta(p) = 1$ und $\beta(q) = 1$; kein Modell ist die Belegung $\beta(p) = 1$ und $\beta(q) = 0$.
2. Die Formel $p \to (q \to r)$ ist weder eine Tautologie noch eine Kontradiktion. Ein Modell ist die Belegung, die alle Variablen auf 1 setzt; kein Modell ist die Belegung $\beta(p) = 1$ und $\beta(q) = 1$ und $\beta(r) = 0$.
3. Die Formel $(p \lor \neg p) \land (q \lor \neg q) \land (r \lor \neg r)$ ist eine Tautologie.

Lösung zu 2.13

1. Diese Formel ist eine Kontradiktion.
2. Diese Formel ist weder eine Tautologie noch eine Kontradiktion. Ein Modell ist die Belegung $\beta(a) = 1$, $\beta(b) = 1$, $\beta(c) = 1$; kein Modell ist die Belegung $\beta(a) = 1$, $\beta(b) = 0$, $\beta(c) = 0$.
3. Diese Formel ist weder eine Tautologie noch eine Kontradiktion. Ein Modell ist die Belegung $\beta(a) = 1$, $\beta(b) = 0$, $\beta(c) = 0$; kein Modell ist die Belegung $\beta(a) = 0$, $\beta(b) = 1$, $\beta(c) = 1$.

3-1

Kapitel 3
Semantische Folgerung
Wenn Wenn-Dann, dann Wenn-Dann

3-2

Lernziele dieses Kapitels

1. Die Begriffe der semantischen Folgerung und Äquivalenz kennen
2. Formeln auf Äquivalenz und Folgerungsbeziehungen untersuchen können
3. Beweisebenen bei Beweisen über Logik trennen können

Inhalte dieses Kapitels

Worum es heute geht

Der Merowinger bemerkt im zweiten Teil der Matrix treffend, wenn auch leicht französisch näselnd: »You see, there is only one constant, one universal, it is the only real truth: causality. Action. Reaction. Cause and effect.« In der Tat ist die Welt schwierig ohne Kausalität zu erklären, ohne Wenn-Dann, ohne »Wer A sagt, muss auch B sagen.« Andererseits sollten Sie sich vom Geschwafel des Merowingers auch nicht zu sehr einlullen lassen und Bertolt Brechts Bemerkung »Wer A sagt, der muss nicht B sagen. Er kann auch erkennen, dass A falsch war.« beachten. Wieder ist es eine der großen philosophischen Fragen, wie man Kausalität genau definieren sollte und warum es sie überhaupt gibt (dies ist übrigens eine Frage nach der Kausalität der Kausalität – ich denke, Sie sehen, warum die Philosophen diese Frage für vertrackt halten). Wieder wollen wir die Grundsatzprobleme den Philosophen überlassen und uns auf die mathematische Ebene(n) konzentrieren.

Jedoch selbst in der Mathematik steckt mehr hinter Wenn-Dann als der einfache Implikations-Junktor ($\rightarrow$), den wir bis jetzt auf der syntaktischen Ebene kennengelernt haben. In diesem Kapitel geht es um die Idee des »Wenn-Dann« auf zwei neuen Ebenen: der semantischen und der Meta-Ebene.

Beginnen wir mit einem Praxisbeispiel. Beim Amt für Problemlösungen gibt es genau zwei Tage, an denen man Anliegen vorbringen darf: *Montage* und *Freitage*. Es gibt auch nur zwei Anliegen, die man vortragen darf: *Probleme*, die dann vom Amt gelöst werden, und *Beschwerden*, die dann vom Amt ignoriert werden. Der Leiter des Amtes, Herr Winston Wolf, hat im Foyer einige Hinweise aufgestellt, wann man sich mit welchen Anliegen an das Amt wenden kann:

1. Um die Arbeitslast unser Sachbearbeiter gering zu halten, können an einem Freitag leider keine Beschwerden vorgebracht werden, wenn am Montag bereits eine Beschwerde vorgebracht wurde.
2. Leider ist es uns nicht möglich, am Montag sowohl eine Beschwerde wie ein Problem entgegenzunehmen.
3. Zur Verbesserung der Qualität müssen am Montag vorgebrachte Beschwerden am Freitag noch einmal vorgebracht werden, damit sie nicht verloren gehen.

In diesen Hinweisen stecken schon einige »Wenn-Dann«-Bedingungen wie »wenn die Aussage *Beschwerde am Montag eingereicht* wahr ist, dann auch die Aussage *Beschwerde am Freitag eingereicht*«, was Sie mittlerweile auch vorbildlich als Formel aufschreiben könnten, also *syntaktisch* kodieren könnten.

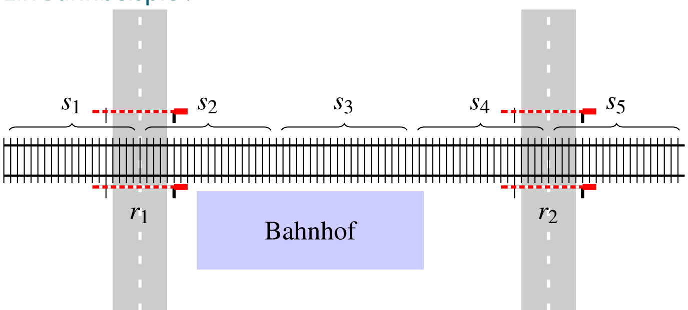
In diesem Kapitel soll es nun aber um Wenn-Dann-Bedingungen »einer Ebene höher« gehen. Hier ein Beispiel: Mit etwas Nachdenken wird man feststellen, dass immer, *wenn* man die Regeln einhält, *dann* Montag als Beschwerdetag ausscheidet. Beachten Sie, dass dies keine »Wenn-Dann«-Regel wie die anderen ist, denn hier wird keine neue Regel aufgestellt, sondern etwas *über die Welten* ausgesagt, in denen diese Regeln gelten. Wenn-Dann-Beziehungen, die etwas darüber aussagen, in welche Welten bestimmte Formeln gelten, werden wir *semantische Folgerungen* nennen, da es hier um Welten (also die Semantik) von Formeln geht.

Das Spiel kann man natürlich weitertreiben. Der nächste Schritt ist nun, eine Wenn-Dann-Beziehung zwischen semantischen Folgerungen aufzustellen oder auch zwischen semantischen und syntaktischen Folgerungen. Diese Ebene nennt man die *Meta-Ebene*. Und, wenig verwunderlich, es gibt natürlich auch noch eine Meta-Meta-Ebene und so weiter. Argumente auf diesen höheren Ebenen werden dann aber irgendwann ein wenig *silly* wie der Engländer sagen würde, weshalb wir bei der Meta-Ebene Schluss machen werden.

3.1 Der Folgerungsbegriff

3.1.1 Semantische Folgerung

Ein Bahnbeispiel. 3-5



Der TÜV muss prüfen, dass *für alle physikalisch möglichen Welten* β gilt:

$$\beta \models ((s_1 \vee s_2) \to r_1) \wedge ((s_4 \vee s_5) \to r_2)$$

Eine (dumme) Beschaltung wäre, dass die Schranken runtergehen, wenn irgendein Sensor anspricht. Die *physikalisch möglichen Welten* sind dann genau die Welten β, die Modelle der Formel $(s_1 \vee (s_2 \vee (s_3 \vee (s_4 \vee s_5)))) \to (r_1 \wedge r_2)$ sind.

Die semantische Folgerung. 3-6

In unserem Beispiel beschreibt *eine Formel* die *Welten*, für die etwas überprüft werden soll. Eine *zweite Formel* beschreibt, was wir überprüfen sollen.

▶ Definition: Semantische Folgerung für einzelne Aussagen

Seien φ und ψ Formeln (Elemente von $L_{\text{Aussagenlogik}}$). Wir schreiben

$$\psi \models \varphi,$$

falls für jede Welt, die sowohl für ψ wie für φ zulässig ist, gilt: Ist sie ein Modell von ψ, so auch von φ.

Statt $\mathtt{w} \models \varphi$ schreiben wir auch $\models \varphi$.

Beispiel: Was der TÜV überprüfen muss

$$\begin{aligned}&(s_1 \vee (s_2 \vee (s_3 \vee (s_4 \vee s_5)))) \to (r_1 \wedge r_2)\\ \models\ &((s_1 \vee s_2) \to r_1) \wedge ((s_4 \vee s_5) \to r_2)\end{aligned}$$

3.1.2 Folgerung und Implikation

3-7 Zusammenhang zwischen Folgerung und Implikations-Junktor.

▶ Satz
Seien ψ und φ Formeln. Dann gilt $\psi \models \varphi$ genau dann, wenn $(\psi \to \varphi) \in \textsc{taut}$.

3-8 Beweisrezept: *Zwei Beweisrichtungen*

Ziel
Es soll gezeigt werden, dass eine Behauptungen A genau dann gilt, wenn eine andere Behauptung B gilt.

Rezept
Zeige, dass die Aussagen sich gegenseitig implizieren:

1. Beginne mit »Es sind zwei Richtungen zu zeigen.«
2. Fahre fort mit »Für die erste Richtung nehmen wir an, dass A gilt.« Folgere, dass dann auch B gelten muss.
3. Beginne einen neuen Absatz mit »Für die Rückrichtung nehmen wir an, dass B gilt.« Folgere, dass dann auch A gelten muss.

3-9 Beweis des Satzes.

Beweis. Es sind zwei Richtungen zu zeigen.[1]
Für die erste Richtung nehmen wir an, dass $\psi \models \varphi$ gilt. Wir wollen zeigen, dass $(\psi \to \varphi)$ eine Tautologie ist.[2] Sei β eine beliebige Welt. Falls $\hat\beta(\psi) = 0$, so gilt $\hat\beta(\psi \to \varphi) = 1$. Falls $\hat\beta(\psi) = 1$, so folgt aus $\psi \models \varphi$, dass $\hat\beta(\varphi) = 1$ gilt. Also gilt wieder $\hat\beta(\psi \to \varphi) = 1$.[3]
Für die Rückrichtung sei nun $(\psi \to \varphi)$ eine Tautologie.[4] Wir wollen zeigen, dass $\psi \models \varphi$ gilt. Sei β ein Modell von ψ. Das bedeutet $\hat\beta(\psi) = 1$. Da $\hat\beta(\psi \to \varphi) = 1$ gilt – schließlich ist $(\psi \to \varphi)$ eine Tautologie – folgt $\hat\beta(\varphi) = 1$.[5] Also ist β ein Modell von φ. □

Kommentare zum Beweis

[1] Originaltexte aus dem Rezept.

[2] Hier steht für den Leser vorsichtshalber nochmal, was gerade »B« ist.

[3] Da es nur zwei mögliche Fälle gibt, ist »B« gezeigt.

[4] Originaltext aus dem Rezept.

[5] Vergleiche die Definitionen.

3.1.3 Die zwei Beweisebenen

3-10 Die zwei Argumentationebenen im Beweis.
Im Beweis von eben kann man *zwei Ebenen* unterscheiden:

1. Im Beweis wird *über Logik geredet*. Es geht um *Formeln* und *Modelle* und so weiter.
2. Im Beweis wird *mit logischen Argumenten etwas bewiesen*. Es gibt Formulierungen wie »Falls …, so gilt …« oder »also folgt«.
   Diese zweite Ebene nennt man manchmal *Metaebene*.

Wir benutzen Logik, um etwas über Logik zu zeigen.

3-11 Beweisrezept: *Trennung der Ebenen*

Ziel
Die zwei Beweisebenen sollen dem Leser klar werden.

Rezept

1. Für die »Objekte der Logik« benutzen wir *Formeln* und *Symbole*.
2. Für die Metaebene benutzen wir *normalsprachlichen Text*.

Beispiel: Gute Schreibweise
… Falls $\hat\beta(\psi) = 0$, so gilt $\hat\beta(\psi \to \varphi) = 1$. …

Beispiel (Schlechte Schreibweise)
… $\hat\beta(\psi) = 0 \to \hat\beta(\psi \to \varphi) = 1$. …

✎ Zur Übung 3-12

Korrigieren Sie die folgenden Formulierungen:

1. »Seien ψ und φ Formeln, sei $\rho = (\psi \wedge \varphi)$, sei $\beta(\varphi)$ wahr $\wedge$ sei $\beta(\psi) = 1$. Dann ...«
2. »Sei ψ eine Formel. $\implies$ für alle Variablen v in ψ gilt...«
3. »Es gilt $\forall \psi \in L_{\text{Aussagenlogik}}$, dass ψ nur dann ...«

Die drei Bedeutungen von »daraus folgt« im Beweis. 3-13

Im Beweis wird »daraus folgt« auf drei Arten verwendet:

1. Als Implikations-Junktor (geschrieben »$\rightarrow$«). Dies ist ein Teil der *Syntax der Aussagenlogik*.
   Der Implikations-Junktor stellt *syntaktische Beziehungen zwischen verschiedenen Formelteilen her*.
2. Als Folgerungsrelation (geschrieben »$\models$«). Dies ist ein Teil der *Semantik der Aussagenlogik*.
   Hier werden *semantische Beziehungen zwischen verschiedenen Formeln hergestellt*.
3. Als Teil des Beweises selber (geschrieben »daraus folgt«). Dies ist Teil einer *Argumentation auf der Metaebene*, in der etwas *über Logik* gezeigt wird.

Erweiterung der Definition auf Formelmengen. 3-14

Genau wie beim Modellbegriff für viele Formeln können wir einen Folgerungsbegriff für Formelmengen definieren.

▶ Definition: Semantische Folgerung für Formelmengen

Seien Φ und Ψ Mengen von Formeln. Wir schreiben

$$\Psi \models \Phi,$$

falls für jede Welt, die sowohl für Ψ wie auch für Φ zulässig ist, gilt: Ist sie ein Modell von Ψ, so auch von Φ.

Beispiel

Es gilt $\{\neg h \vee s, h\} \models s \wedge h$:
Für jeden Planeten (wie der Erde), auf dem es (a) kein Wasser gibt oder der um die Sonne kreist und es (b) Wasser gibt, gilt, dass es Wasser gibt und er sich um die Sonne bewegt.

✎ Zur Übung 3-15

Lösen Sie *eine* der folgenden, nach Schwierigkeit sortierten Aufgaben:

1. Gilt $(p \wedge q) \models (p \vee q)$?
2. Gilt $\{(q \rightarrow r), (p \rightarrow q)\} \models \{(p \rightarrow r)\}$?
3. Gilt $\{(q \rightarrow r), (p \rightarrow q)\} \models \{(p \rightarrow s)\}$?
4. Gilt $\{a_1 \leftrightarrow \neg a_2, a_2 \leftrightarrow \neg a_3, a_3 \leftrightarrow \neg a_4, \dots\} \models \{a_1\}$?

3.1.4 Wichtige Folgerungen

Wichtige Folgerungen. 3-16

▶ Satz

Seien φ und ψ Formeln. Dann gelten:

1. *Modus ponens:*
   $\varphi \wedge (\varphi \rightarrow \psi) \models \psi$
2. *Kettenschluss:*
   $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \rho) \models (\varphi \rightarrow \rho)$
3. *Reductio ad absurdum:*
   $(\varphi \rightarrow \psi) \wedge \neg \psi \models \neg \varphi$
4. *Abschwächung der Annahme:*
   $\varphi \wedge \psi \models \varphi$
5. *Abschwächung der Folgerung:*
   $\varphi \models \varphi \vee \psi$

3-17 **Beweisrezept:** *Wahrheitstafeln für Tautologien*

Ziel

Zeigen, dass eine Formel eine Tautologie ist.

Rezept

1. Identifiziere alle vorkommenden Variablen oder geeignete Teilformeln.
2. Für jede mögliche Kombination von Wahrheitswerten der Variablen oder Teilformeln verifiziere, dass die Formel zu wahr auswertet.

3-18 **Beweis der wichtigen Implikationen.**

Beweis einer der Folgerungen. Als Beispiel wollen wir zeigen, dass $\varphi \wedge (\varphi \to \psi) \models \psi$. Dazu muss man zeigen, dass $(\varphi \wedge (\varphi \to \psi)) \to \psi$ eine Tautologie ist.
Es ergeben sich folgende Möglichkeiten:

$\hat\beta(\varphi)$	$\hat\beta(\psi)$	$\hat\beta((\varphi \wedge (\varphi \to \psi)) \to \psi)$
0	0	1
0	1	1
1	0	1
1	1	1

□

3.2 Semantische Äquivalenz

3.2.1 Idee

3-19 **Geht es auch ein bisschen einfacher?**

Sie lesen in einem Schreiben:

> Nur dann gilt keine der Fristen als versäumt, wenn der Antrag nicht später als bis zum Jahresende gestellt wird.

Was man wohl besser hätte schreiben sollen:

> Der Antrag muss bis Jahresende gestellt werden.

3-20 **Geht es auch ein bisschen einfacher?**

Sie lesen in die Formel:

$$\neg\neg(\neg\neg a \to \neg\neg\neg b)$$

Was man wohl besser hätte schreiben sollen:

$$a \to \neg b$$

3-21 **Die semantische Äquivalenz.**

Manche Formeln sind einfach nur »Umformulierungen« anderer Formeln. Genauer haben diese Formeln genau dieselben Modelle.

▶ **Definition:** Semantische Äquivalenz

Seien ψ und φ zwei Formeln. Wir schreiben

$$\psi \equiv \varphi,$$

falls für jede Welt, die sowohl für ψ wie auch für φ zulässig ist, gilt: Sie ist ein Modell von ψ genau dann, wenn sie ein Modell von φ ist.

Beispiele

- $(p \wedge q) \equiv (q \wedge p)$
- $\neg\neg p \equiv p$.

3.2.2 Äquivalenz ist äquivalent zu Äquivalenz

Alternative Charakterisierungen der Äquivalenz. 3-22

Satz
Seien φ und ψ Formeln. Dann sind die folgenden Aussagen äquivalent:

1. $\varphi \equiv \psi$
2. $\varphi \models \psi$ *und* $\psi \models \varphi$
3. $(\varphi \leftrightarrow \psi) \in \text{TAUT}$

Beweisrezept: *Kreisschluss* 3-23

Ziel
Es soll gezeigt werden, dass mehrere Behauptungen gleichwertig sind.

Rezept
Zeige, dass die Aussagen sich kreisförmig implizieren. Dies geschieht wie folgt:

1. Nimm an, dass die erste Aussage gilt. Folgere, dass nun auch die zweite gelten muss.
2. Beginne nun eine neue Argumentation. Nimm an, dass die zweite Aussage gilt. Folgere, dass dann die dritte gelten muss.
3. Und so weiter bis zur letzte, für die man zeigt, dass sie die erste impliziert.

Falls nun eine Aussage gilt, so gelten folglich alle.

Beweis des Satzes über die Charakterisierungen. 3-24

Beweis. Die erste Aussage impliziert die zweite:[1] Aus $\varphi \equiv \psi$ folgen sowohl $\varphi \models \psi$ als auch $\psi \models \varphi$, denn falls φ und ψ genau dieselben (zulässigen) Modelle haben, so ist jedes Modell von φ ein Modell von ψ und umgekehrt.
Als nächstes zeigen wir, dass, falls $\varphi \models \psi$ und $\psi \models \varphi$ gelten, so auch $(\varphi \leftrightarrow \psi) \in \text{TAUT}$.[2]
Wir wissen schon, dass aus $\varphi \models \psi$ folgt $(\varphi \rightarrow \psi) \in \text{TAUT}$.[3] Ebenso folgt aus $\psi \models \varphi$, dass $(\psi \rightarrow \varphi) \in \text{TAUT}$. Also sind $(\varphi \rightarrow \psi)$ und $(\psi \rightarrow \varphi)$ Tautologien. Hieraus folgt $(\varphi \leftrightarrow \psi) \in \text{TAUT}$.[4]
Wir zeigen nun noch, dass die dritte Aussage die erste impliziert. Nehmen wir nämlich an, dass $(\varphi \leftrightarrow \psi) \in \text{TAUT}$ gilt. Wir wollen zeigen, dass $\varphi \equiv \psi$ gilt.[5]
Sei dazu β ein Modell von φ.[6] Dann gilt $\hat\beta(\varphi) = 1$. Wegen $(\varphi \leftrightarrow \psi) \in \text{TAUT}$ gilt ebenfalls $\hat\beta(\varphi \leftrightarrow \psi) = 1$. Nach der Definition von $\hat\beta$ für den Äquivalenz-Junktor folgt nun $\hat\beta(\psi) = 1$. Also ist β ein Modell von ψ.
Sei als nächstes β ein Modell von ψ.[7] Wir argumentieren genauso, um zu zeigen, dass β ein Modell von φ ist, nur mit den Rollen von ψ und φ vertauscht. □

Kommentare zum Beweis

[1] Hier wird angedeutet, dass jetzt ein Kreisschluss beginnt.

[2] Der Kreisschluss geht weiter.

[3] Das war vorhin ein Satz.

[4] Dass das folgt, wird in Übungsaufgabe 3.2 gezeigt.

[5] Es schadet nie, das Ziel nochmal hinzuschreiben.

[6] Nach der Definition von $\varphi \equiv \psi$ sind zwei Richtungen zu zeigen. Hier die erste. . .

[7] . . . und die zweite.

3.2.3 Wichtige Äquivalenzen

Wichtige Äquivalenzen 3-25

Satz
Seien φ, ψ und ρ Formeln. Dann gelten die folgenden Äquivalenzen:

1. *Kommutativität des Und-Junktors, des Oder-Junktors und des Äquivalenz-Junktors:*
   $\varphi \wedge \psi \equiv \psi \wedge \varphi$, $\varphi \vee \psi \equiv \psi \vee \varphi$ *und* $\varphi \leftrightarrow \psi \equiv \psi \leftrightarrow \varphi$
2. *Idempotenz:*
   $\varphi \wedge \varphi \equiv \varphi$ *und* $\varphi \vee \varphi \equiv \varphi$.
3. *Doppelte Negation:*
   $\neg\neg\varphi \equiv \varphi$
4. *Kontraposition:*
   $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$
5. *Absorption:*
   $\varphi \vee (\varphi \wedge \psi) \equiv \varphi$ *und* $\varphi \wedge (\varphi \vee \psi) \equiv \varphi$

7. *Assoziativität:*
   $\varphi \vee (\psi \vee \rho) \equiv (\varphi \vee \psi) \vee \rho$ *und* $\varphi \wedge (\psi \wedge \rho) \equiv (\varphi \wedge \psi) \wedge \rho$
8. *Distributivität:*
   $\varphi \wedge (\psi \vee \rho) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \rho)$ *und* $\varphi \vee (\psi \wedge \rho) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \rho)$
9. *De Morgan'sche Regeln:*
   $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ *und* $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$

Zusammenfassung dieses Kapitels

3-26 ▶ Semantische Folgerung
Wir schreiben $\varphi \models \psi$, wenn jedes Modell von φ auch ein Modell von ψ ist.

▶ Satz
Seien φ und ψ Formeln. Dann sind äquivalent:

1. $\psi \models \varphi$.
2. $(\psi \to \varphi) \in \text{TAUT}$.

▶ Wichtige semantische Folgerungen

Modus ponens $\varphi \wedge (\varphi \to \psi) \models \psi$

Kettenschluss $(\varphi \to \psi) \wedge (\psi \to \rho) \models (\varphi \to \rho)$

Reductio ad absurdum $(\varphi \to \psi) \wedge \neg\psi \models \neg\varphi$

Annahmen-Abschwächung $\varphi \wedge \psi \models \varphi$

Folgerungs-Abschwächung $\varphi \models \varphi \vee \psi$

▶ Semantische Äquivalenz
Wir schreiben $\varphi \equiv \psi$, wenn φ und ψ dieselben Modell haben.

▶ Satz
Seien φ und ψ Formeln. Dann sind äquivalent:

1. $\psi \equiv \varphi$.
2. $\varphi \models \psi$ und $\psi \models \varphi$.
3. $(\psi \leftrightarrow \varphi) \in \text{TAUT}$.

▶ Wichtige semantische Äquivalenzen

Kommutativität $\varphi \wedge \psi \equiv \psi \wedge \varphi$ und $\varphi \vee \psi \equiv \psi \vee \varphi$

Assoziativität $((\varphi \wedge \psi) \wedge \rho) \equiv (\varphi \wedge (\psi \wedge \rho))$ und $((\varphi \vee \psi) \vee \rho) \equiv (\varphi \vee (\psi \vee \rho))$

Kontraposition $\varphi \to \psi \equiv \neg\psi \to \neg\varphi$

De Morgan'sche Regel $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ und $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$

Übungen zu diesem Kapitel

Übung 3.1 Beweisrezepte anwenden, schwer

Seien φ_1, φ_2 und ψ jeweils aussagenlogische Formeln. Zeigen Sie: $\{\varphi_1, \varphi_2\} \models \psi$ gilt genau dann, wenn $\varphi_1 \wedge \varphi_2 \models \psi$ gilt.

Übung 3.2 Beweisrezepte anwenden, mittel

Seien φ und ψ aussagenlogische Formeln. Zeigen Sie: Aus $\models \{(\varphi \to \psi), (\psi \to \varphi)\}$ folgt $\models (\varphi \leftrightarrow \psi)$.

Übung 3.3 Alternative Junktoren, mittel

Neben den Junktoren $\neg$, $\vee$, $\wedge$, $\to$ und $\leftrightarrow$ kann man auch noch weitere definieren. Beispielsweise ist die Auswertungsfunktion $\hat{\beta}$ für die Junktoren $\oplus$ und nand folgendermaßen definiert:

$$\hat{\beta}(\psi \oplus \rho) = \begin{cases} 1, & \text{falls } \hat{\beta}(\psi) \neq \hat{\beta}(\rho), \\ 0, & \text{sonst.} \end{cases}$$

$$\hat{\beta}(\psi \operatorname{nand} \varphi) = 1 - \hat{\beta}(\psi \wedge \varphi).$$

Geben Sie für die folgenden aussagenlogischen Formeln äquivalente Formeln an, die als Junktoren nur $\neg$ und nand enthalten.

1. $a \vee y$
2. $a \to y$
3. $a \leftrightarrow y$
4. $a \oplus y$

Übung 3.4 Alternative Junktoren, mittel

Geben Sie für die folgenden aussagenlogischen Formeln äquivalente Formeln an, die als Junktor nur nand enthalten (siehe zur Definition die vorherige Aufgabe).

1. $\neg x$
2. $x \vee y$
3. $x \wedge y$
4. $x \to y$
5. $x \leftrightarrow y$

Übung 3.5 Semantische Beziehungen zwischen Formeln, mittel

Untersuchen Sie die Äquivalenz und Folgerungsbeziehungen der folgenden Formeln. Geben dazu ein Diagramm an, aus dem für jedes Paar von Formeln hervorgeht, ob sie äquivalent sind, eine Formel semantisch aus der anderen Formel folgt, oder keine dieser Beziehungen zutrifft.

1. $\neg x \leftrightarrow c$
2. $x \wedge b \to \mathtt{f}$
3. $\neg c \to x$
4. $(x \to b) \to \mathtt{w}$
5. $c \to \neg x$
6. $\neg x \vee \neg b$
7. $\mathtt{f} \wedge b$
8. $\neg b$

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

15 min

Prüfungsfrage 3.6 Alternative Junktoren

Die Auswertungsfunktion $\hat{\beta}$ für den neuen Junktor »nor« ist folgendermaßen definiert:

$$\hat{\beta}(\psi \operatorname{nor} \rho) = 1 - \max\{\hat{\beta}(\psi), \hat{\beta}(\rho)\}.$$

Geben Sie für die folgenden aussagenlogischen Formeln äquivalente Formeln an, die als Junktor nur nor enthalten.

1. $\neg x$
2. $x \vee y$
3. $x \wedge y$
4. $x \to y$
5. $x \leftrightarrow y$

4-1

Kapitel 4
Normalformen

Keep it simple.

4-2

Lernziele dieses Kapitels

1. Wahrheitstafeln kennen und anwenden können
2. Disjunktive und konjunktive Normalform kennen
3. Formeln in Normalformen umwandeln können

Inhalte dieses Kapitels

Worum es heute geht

Denselben Sachverhalt kann man auf verschiedene Weisen ausdrücken. Es gibt also unterschiedliche Arten, ein und dieselbe Sache zu formulieren. Mit anderen Worten, Dinge können so oder so gesagt werden. Damit ist gemeint, dass sich Aussagen drehen und wenden lassen, ohne sie zu ändern. Insbesondere stimmt es nicht, dass es nur eine Möglichkeit gibt, etwas auszusprechen. This means that there are different ways of saying the same thing. Phrased differently, there is an endless supply of different formulations for a single thought. . .

Ohne die Möglichkeit, Dinge auf verschiedene Arten auszudrücken, wäre die Literatur wahrlich fade und öde. Sprache lebt davon, dass man mit ihr spielt, dass man durch geschickte Wendungen und Formulierungen Akzente setzt, den Dingen Leben einhaucht.

Was für die Lyrik gut ist, muss nicht unbedingt auch für die Informatik und die Logik wohltuend sein. Java-Programme und aussagenlogische Formeln sind schließlich keine Liebesgedichte (wobei `while(true)System.out.print("I love you. ");` der Sache schon recht nahe kommt).

Bei logischen Formeln ist es oftmals sehr natürlich danach zu fragen, ob man nicht eine einfachere Formulierung für eine gegebene Formel finden kann. Ein klassisches Beispiel ist die doppelte Verneinung, die man einfach weglassen kann: Statt »Es ist nicht der Fall, dass es nicht der Fall ist, dass a gilt« kann man auch einfacher sagen »a gilt«. Mathematisch geschrieben: $\neg\neg a \equiv a$. Es gibt aber auch komplexere Fälle, die nicht so offensichtlich sind: »Es ist nicht der Fall, dass nicht a und auch nicht b gelten« lässt sich auch schreiben als »a oder b«, mathematisch $\neg(\neg a \wedge \neg b) \equiv a \vee b$.

In diesem Kapitel geht es darum, was passiert, wenn man solche Vereinfachungen bis zum bitteren Ende durchführt. Dabei ist zunächst gar nicht klar, wo denn das bittere Ende sein wird. Gibt es Formeln, die sich nicht weiter vereinfachen lassen? Sicherlich wird die doch recht minimalistische Formel a diese Eigenschaft haben. Genauso aber auch $a \vee b$, es geht wirklich nicht simpler. Bei einer Formel wie $(a \vee b) \wedge (c \vee d)$ ist aber schon nicht mehr klar, ob hier jetzt das Ende der Fahnenstange erreicht ist.

Normalformen sind »Formen von Formeln«, die einen solchen Zustand der maximalen Vereinfachung erreicht haben. Originellerweise gibt es gleich zwei Arten von Normalformen für aussagenlogische Formeln: die disjunktive Normalform und die konjunktive Normalform. Dass es zwei Arten gibt, liegt nicht daran, dass sich ein Normierungsgremium nicht einigen konnte, sondern daran, dass es eben auf den Standpunkt oder die Anwendung ankommt, was die »einfachste« Fassung einer Formel ist.

Das Konzept, Dinge so lange zu vereinfachen bis etwas »in Normalform« herauskommt, wird Ihnen in Ihrem Studium noch häufig begegnen. Sie werden Normalformen für reguläre Grammatiken kennen lernen, mehrere Normalformen für kontextfreie Grammatiken, ja sogar Normalformen für Computerprogramme. Das Studium der Normalformen bringt dabei manchmal etwas wunderliche Resultate hervor – wenn Sie beispielsweise verschachtelte Schleifen nicht mögen, so wird es sie sicherlich beruhigen zu erfahren, dass Sie jedes Javaprogramm so »vereinfachen« können, dass alle While- und For-Schleifen durch eine einzige While-Schleife ersetzt werden.

4.1 Einführung

Wiederholung: Geht es auch ein bisschen einfacher? 4-4

Folgende Sätze sind *syntaktisch unterschiedlich* aber *semantisch äquivalent*:

1. *»Nur dann gilt keine der Antragsfristen als versäumt, wenn der Antrag nicht später als bis zum Jahresende gestellt wird.«*
2. *»Der Antrag muss bis Jahresende gestellt werden.«*

✎ Zur Übung 4-5

Lernkontrolle zu semantischer Äquivalenz: Welche der folgenden Behauptungen stimmen?

1. »$\varphi \equiv \psi$« bedeutet, dass φ und ψ genau dieselben Modelle haben.
2. »$\varphi \equiv \psi$« bedeutet, dass φ ein Modell von ψ ist und auch ψ ein Modell von φ ist.
3. $\varphi \wedge \psi \equiv \psi \wedge \varphi$
4. $\varphi \to \psi \equiv \psi \to \varphi$

4.1.1 Motivation mit Schafen

Schafe I: Welcher Satz sagt etwas anderes als die anderen beiden? 4-6

1. Dolly ist weiß und Max ist schwarz.
2. Wenn Dolly nicht weiß ist, dann ist Max schwarz.
3. Es stimmt nicht, dass, wenn Dolly weiß ist, Max nicht schwarz ist.

Schafe II: Welcher Satz sagt etwas anderes als die anderen beiden? 4-7

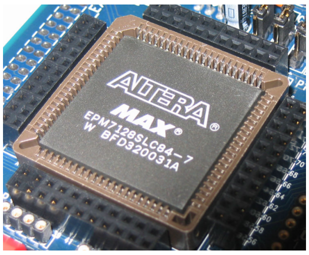
1. Dolly ist weiß und Max ist schwarz.
2. Dolly ist weiß oder Max ist schwarz.
3. Dolly ist weiß und Max ist schwarz.

Die Idee hinter Normalformen. 4-8

Formeln *in Normalform* sind besonders einfach und einheitlich aufgebaut, wobei es *verschiedene Arten von Normalformen* gibt. Formeln in Normalform kann man oft *leichter verarbeiten*, beispielsweise kann man oft *leichter Erfüllbarkeit oder Äquivalenz testen*.
Eine *Formel φ in Normalform umwandeln* bedeutet, eine zu φ äquivalente Formel in Normalform zu finden.

4.1.2 Motivation mit Chips

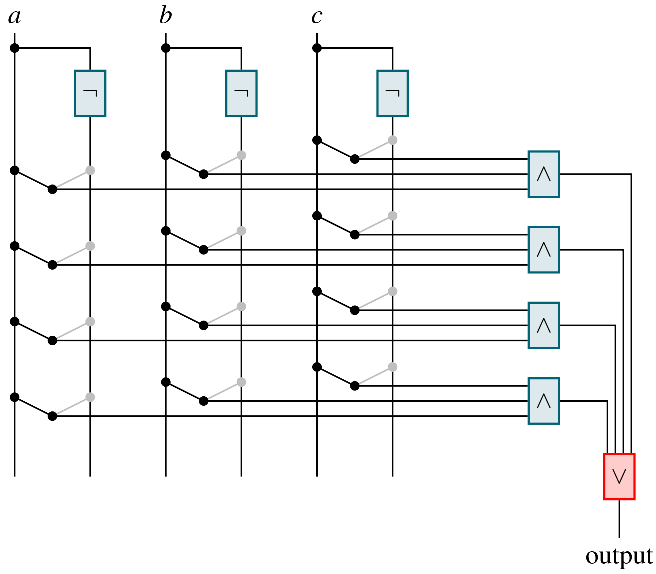
4-9 **Normalformen und Chips.**



Unknown author, public domain

1. Ein CPLD (Complex Programmable Logic Device) ist ein Chip.
2. An einigen Pins kommen Wahrheitswerte hinein (ein β), an einem kommt $\hat\beta(\varphi)$ heraus.
3. Die Verdrahtung lässt sich zur Laufzeit *umkonfigurieren*.
4. Dies geht aber *nicht beliebig*, weshalb sich nur φ *in einer bestimmten Normalform* konfigurieren lassen.

4-10 **Eine konfigurierbare Verdrahtung auf einem Chip.**



4.2 Disjunktive Normalform

4.2.1 Definition

4-11 **Monome**

▶ **Definition:** Literal
Ein *Literal* ist eine Variable oder eine negierte Variable.

▶ **Definition:** Monom
Ein *Monom* ist eine Formel, die nur aus durch Und-Junktoren verbundenen Literalen besteht. Weiterhin ist auch w ein Monom (das »leere« Monom).

Beispiele

1. $a \wedge \neg b \wedge c \wedge \neg d$
2. $\neg a \wedge \neg b$
3. $b \wedge c \wedge a$
4. $\neg a$

Bemerkungen zur Schreibweise:

- Andere übliche Schreibweisen von $\neg x$ sind $\bar{x}$ sowie x^0.
- Statt $x \wedge y \wedge z$ schreibt man manchmal auch xyz.

4-12 ✎ **Zur Übung**
Finden Sie zu folgenden Formeln jeweils ein äquivalentes Monom (bei einer Formel ist dies nicht möglich):

1. $\neg(a \vee b)$
2. $\neg(a \rightarrow b)$
3. $\neg\neg a \vee b$

Formeln in disjunktiver Normalform. 4-13

Definition: Disjunktive Normalform

Eine Formel ist *in disjunktiver Normalform*, falls sie nur aus durch Oder-Junktoren verbundenen Monomen besteht.

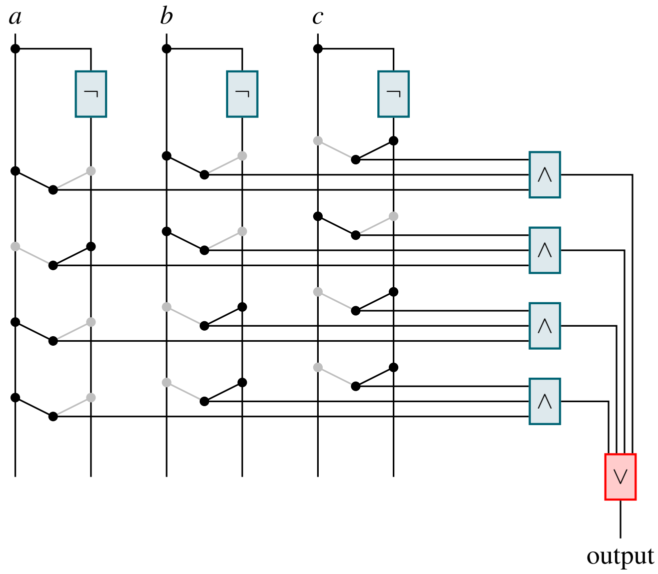
Beispiel

$$\underbrace{\underbrace{(a \wedge \neg b \wedge \neg a)}_{\text{Monom}} \vee \underbrace{(b \wedge \neg c \wedge d)}_{\text{Monom}} \vee \underbrace{(\neg c)}_{\text{Monom}} \vee \underbrace{(c \wedge b)}_{\text{Monom}}}_{\text{Oder-Junktoren außerhalb der Klammern}}$$

Merke

1. Disjunktion = Oder
2. Die *disjunktive* Normalform heißt so, weil die *Oder*-Junktoren die Strukturierung auf der *äußersten* Ebene darstellen.

$(a \wedge b \wedge \neg c) \vee (\neg a \wedge b \wedge c) \vee (a \wedge \neg b \wedge \neg c)$ verdrahtet. 4-14



4.2.2 Existenz

Man kann jede Formel in disjunktive Normalform umwandeln. 4-15

Satz

Zu jeder aussagenlogischen Formeln φ gibt es eine Formel φ' mit folgenden Eigenschaften:

1. *φ' ist in disjunktiver Normalform.*
2. *$\varphi \equiv \varphi'$*

Bemerkung: Aus dem Beweis wird klar werden, wie φ' berechnet werden kann.

4.2.3 Konstruktion

4-16 **Beweisrezept:** *Konstruktive Beweise*

Ziel

Es soll gezeigt werden, dass es ein Ding mit bestimmten Eigenschaften gibt.

Rezept

1. Beginne den Beweis mit »Wir führen einen konstruktiven Beweis.«
2. Fahre fort mit »Wir konstruieren das . . . wie folgt:« und gebe dann an, wie ein bestimmtes Ding *konstruiert* werden soll.
3. Fahre fort mit »Das konstruierte . . . hat die behaupteten Eigenschaften:« und zeige nun, dass das konstruierte Ding die behaupteten Eigenschaften hat.

Der zweite Schritt wird gerne vergessen!

4-17 **Beweis der Existenz der disjunktiven Normalform.**

Kommentare zum Beweis

[1] Hinweis auf das verwendete Beweisrezept

[2] Es kommt jetzt ein »Inhaltsverzeichnis des Beweises«. Dies ist sehr hilfreich bei langen Beweisen.

Beweis. Wir führen einen *konstruktiven Beweis*.[1] Sei φ eine Formel.[2]

1. Wir erstellen die *Wahrheitstafel* für φ. Hieraus *konstruieren* wir die Formel φ' (dazu gleich mehr).
2. Es bleiben die *behaupteten Eigenschaften* von φ' nachzuweisen. Aus der Konstruktion wird klar sein, dass φ' in disjunktiver Normalform ist. Wir zeigen dann noch, dass $\varphi \equiv \varphi'$ gilt (dazu auch gleich mehr).

Wir erstellen die *Wahrheitstafel* für φ. Diese ist wie folgt aufgebaut: Es gibt für *jede in φ vorkommende Variable eine Spalte* sowie eine *Ergebnisspalte*. Es gibt für *jede mögliche Variablenbelegung β* eine Zeile. In ihr stehen die Werte der Variablen sowie $\hat\beta(\varphi)$ in der Ergebnisspalte. Die Formel φ' wird nun wie folgt gebildet:[3] Es gibt für jede Zeile der Wahrheitstafel mit $\hat\beta(\varphi) = 1$ ein Monom in φ'. Ein solches Monom enthält genau ein Literal für jede Variable von φ, wobei genau die Literale negiert sind, für die die Variable in der Zeile 0 ist.

Als Beispiel für die Konstruktion betrachten wir die Formel $\varphi = (\neg a \to b) \wedge (b \wedge c)$.[4]

[3] Hier ist der Teil »Konstruktion« aus dem Beweisrezept.

[4] Beispiele für Konstruktionen sind in Beweisen sehr willkommen, sie helfen den Lesern, die Konstruktion nachzuvollziehen. Allerdings dürfen sie nicht *anstatt* der exakten Beschreibung der Konstruktion gegeben werden, sondern nur *zusätzlich*.

Beispiel: Die Wahrheitstafel

$\beta(a)$	$\beta(b)$	$\beta(c)$	$\hat\beta((\neg a \to b) \wedge (b \wedge c))$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Beispiel: Die Monome

$\beta(a)$	$\beta(b)$	$\beta(c)$	$\hat\beta((\neg a \to b) \wedge (b \wedge c))$	Monom
0	0	0	0	–
0	0	1	0	–
0	1	0	0	–
0	1	1	1	$\neg a \wedge b \wedge c$
1	0	0	0	–
1	0	1	0	–
1	1	0	0	–
1	1	1	1	$a \wedge b \wedge c$

Also: $\varphi' = (\neg a \wedge b \wedge c) \vee (a \wedge b \wedge c)$.

Offenbar ist φ' in disjunktiver Normalform.[5] Es bleibt zu zeigen, dass $\varphi \equiv \varphi'$ gilt. Dazu zeigen wir zwei Richtungen:[6]

1. Jedes Modell von φ ist ein Modell von φ'.
2. Jedes Modell von φ' ist ein Modell von φ.

Für die Hinrichtung[7] zeigen wir, dass jedes Modell von φ ein Modell von φ' ist. Es gelte $\beta \models \varphi$. Dann gilt $\hat\beta(\varphi) = 1$. Also gibt es ein Monom μ innerhalb von φ' für dieses β. Für μ gilt nun $\hat\beta(\mu) = 1$, da alle Literale in μ von β wahr gemacht werden.[8] Da φ' alle seine Monome durch Oder-Junktoren verbindet, folgt $\hat\beta(\varphi') = 1$. Für die Rückrichtung zeigen wir, dass jedes Modell von φ' auch ein Modell von φ ist. Es gelte $\beta \models \varphi'$. Dann muss für mindestens eines der Monome μ gelten, dass $\hat\beta(\mu) = 1$ gilt. Dies bedeutet aber, dass in der Wahrheitstafel von φ die zu β gehörige Zeile eine 1 aufweist.[9] Also ist β ein Modell von φ. □

[5] Hier geht jetzt der Teil »Eigenschaften« aus dem Beweisrezept los.

[6] Hinweis auf das Beweisrezept »Zwei Richtungen«

[7] Stirb endlich!

[8] Das macht man sich am besten am Beispiel klar.

[9] Siehe wieder das Beispiel.

4.3 Konjunktive Normalform

4.3.1 Definition

Die konjunktive Normalform ist die »Umkehrung« der disjunktiven Normalform. 4-18

Bei der *konjunktiven Normalform* vertauschen Und- und Oder-Junktoren die Rollen: Aus einem *Und-Block* wird nun ein *Oder-Block*. Diese Oder-Blöcke nennt man auch *Klauseln*.

Die konjunktive Normalform. 4-19

▶ Definition: Klausel

Eine *Klausel* ist eine Formel, die nur aus durch Oder-Junktoren verbundenen Literalen besteht. Weiterhin ist auch `f` eine Klausel (die »leere« Klausel).

▶ Definition: Konjunktive Normalform

Eine Formel ist *in konjunktiver Normalform*, falls sie nur aus durch Und-Junktoren verbundenen Klauseln besteht.

Beispiel

$$\underbrace{\underbrace{(a \lor \neg b \lor \neg a)}_{\text{Klausel}} \land \underbrace{(b \lor \neg c \lor d)}_{\text{Klausel}} \land \underbrace{(\neg c)}_{\text{Klausel}} \land \underbrace{(c \lor b)}_{\text{Klausel}}}_{\text{Und-Junktoren außerhalb der Klammern}}$$

Merke

1. Konjunktion = Und
2. Die *konjunktive* Normalform heißt so, weil die *Und*-Junktoren die Strukturierung auf der *äußersten* Ebene bilden.

4.3.2 Existenz

Man kann jede Formel in konjunktive Normalform umwandeln. 4-20

▶ Satz

Zu jeder aussagenlogischen Formel φ gibt es eine Formel φ' mit folgenden Eigenschaften:

1. *φ' ist in konjunktiver Normalform.*
2. *$\varphi \equiv \varphi'$*

Beweis. Wir wissen bereits, wie man die disjunktive Normalform von $\neg\varphi$ berechnet. Sei ψ diese disjunktive Normalform. Dann gilt $\neg\varphi \equiv \psi$ und somit $\varphi \equiv \neg\psi$. Wendet man auf $\neg\psi$ aber zweimal die De Morgan'sche Regel an und entfernt doppelte Negationen, so erhält man eine äquivalente Formel und diese ist in konjunktiver Normalform. □

4.3.3 Konstruktion I

4-21 **Beispiel für die Berechnung einer konjunktiven Normalform.**

Beispiel: Die Formel
$\varphi = (\neg(a \wedge \neg c) \vee \neg((\neg c \to b) \vee a))$.

Beispiel: Die DNF von $\neg\varphi$

$\beta(a)$	$\beta(b)$	$\beta(c)$	$\hat{\beta}(\neg\varphi)$	Monom
0	0	0	0	–
0	0	1	0	–
0	1	0	0	–
0	1	1	0	–
1	0	0	1	$(a \wedge \neg b \wedge \neg c)$
1	0	1	0	–
1	1	0	1	$(a \wedge b \wedge \neg c)$
1	1	1	0	–

Also $\neg\varphi \equiv (a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge \neg c)$.

Beispiel: Die KNF von φ
Zweimal De Morgan liefert nun:

$$\begin{aligned}
\varphi &\equiv \neg\neg\varphi \\
&\equiv \neg((a \wedge \neg b \wedge \neg c) \vee (a \wedge b \wedge \neg c)) \\
&\equiv \neg(a \wedge \neg b \wedge \neg c) \wedge \neg(a \wedge b \wedge \neg c) \\
&\equiv (\neg a \vee \neg\neg b \vee \neg\neg c) \wedge (\neg a \vee \neg b \vee \neg\neg c) \\
&\equiv (\neg a \vee b \vee c) \wedge (\neg a \vee \neg b \vee c)
\end{aligned}$$

4.3.4 Konstruktion II

4-23 **Ein weiteres Konstruktionsverfahren für konjunktive Normalformen.**
Das Erstellen der Wahrheitstafel ist häufig mühselig. Oft geht es schneller, *die Formel durch äquivalente Umformungen* »flachzuklopfen«.

Idee des Algorithmus (ohne Beweis)
Eingabe ist eine Formel φ.

1. Ersetze alle Vorkommen von $\varphi \leftrightarrow \psi$ durch $(\varphi \to \psi) \wedge (\psi \to \varphi)$. Dann ersetze alle Vorkommen von $\varphi \to \psi$ durch $\neg\varphi \vee \psi$.
2. Benutze die De Morgan'schen Regeln wiederholt, um die Negations-Junktoren zu den Variablen zu bewegen.
3. Entferne doppelte Negationen.
4. Benutze die Regel $(\varphi \wedge \psi) \vee \rho \equiv (\varphi \vee \rho) \wedge (\psi \vee \rho)$ wiederholt, um die Und-Junktoren nach außen zu treiben.

4-24 **Beispiel für die Berechnung einer konjunktiven Normalform.**

Beispiel: Die Formel
$\varphi = (a \wedge \neg c) \vee \neg(\neg c \to b)$.

Beispiel: Die Schritte

1. Zunächst werden wir den Implaktions-Junktor los:
$$(a \wedge \neg c) \vee \neg(\neg c \to b) \equiv (a \wedge \neg c) \vee \neg(\neg\neg c \vee b)$$
2. Jetzt treiben wir die Negationen zu den Variablen:
$$(a \wedge \neg c) \vee \neg(\neg\neg c \vee b) \equiv (a \wedge \neg c) \vee (\neg\neg\neg c \wedge \neg b)$$

3. Jetzt entfernen wir die doppelten Negationen:

$$(a \wedge \neg c) \vee (\neg\neg\neg c \wedge \neg b) \equiv (a \wedge \neg c) \vee (\neg c \wedge \neg b)$$

4. Jetzt treiben wir die Und-Junktoren nach außen.

$$\begin{aligned}
&(a \wedge \neg c) \vee (\neg c \wedge \neg b) \\
\equiv\ &(a \vee (\neg c \wedge \neg b)) \wedge (\neg c \vee (\neg c \wedge \neg b)) \\
\equiv\ &((a \vee \neg c) \wedge (a \vee \neg b)) \wedge ((\neg c \vee \neg c) \wedge (\neg c \vee \neg b)) \\
\equiv\ &(a \vee \neg c) \wedge (a \vee \neg b) \wedge (\neg c \vee \neg c) \wedge (\neg c \vee \neg b)
\end{aligned}$$

✎ Zur Übung 4-25

Verwandeln Sie folgende Formeln in konjunktive Normalform:

1. $(a \to b) \wedge (b \to c)$
2. $(a \vee b) \wedge (c \vee d)$

Zusammenfassung dieses Kapitels

▶ Bespiele für die wichtigsten Begriffe 4-26

Literal	x, $\neg a$, y, $\neg z$
Monom	$x \wedge y$, $\neg a \wedge y \wedge \neg z$, a, $\mathtt{w}$
Klausel	$x \vee y$, $\neg a \vee y \vee \neg z$, a, $\mathtt{f}$
DNF	$(x \wedge y) \vee (\neg a \wedge y \wedge \neg z) \vee a$, $a \vee b$, $a \wedge b$
KNF	$(x \vee y) \wedge (\neg a \vee y \vee \neg z) \wedge a$, $a \vee b$, $a \wedge b$

▶ Satz

Zu jeder aussagenlogischen Formel gibt es äquivalente Formeln in disjunktiver und auch in konjunktiver Normalform.

Übungen zu diesem Kapitel

Natürliche Zahlen können durch Strings $x_n x_{n-1} \dots x_1 x_0$ mit $x_i \in \{0,1\}$ dargestellt werden (Binärdarstellung). Die von einem solchen String repräsentierte Zahl ist $\sum_{i=0}^{n} x_i \cdot 2^i$. Eine ähnliche Darstellung ist mit Hilfe von aussagenlogischen Variablen a_0, …, a_n und einer Belegung $\beta \colon \{a_0, \dots, a_n\} \to \{0,1\}$ möglich. Die dadurch repräsentierte Zahl $\sum_{i=0}^{n} \beta(a_i) \cdot 2^i$ bezeichnen wir in den folgenden Aufgaben mit $\text{number}_{a_n,\dots,a_0}(\beta)$.

Übung 4.1 Teilbarkeit als Formel, mittel

Entwickeln Sie eine aussagenlogische Formel φ, die angibt, ob die Zahl $\text{number}_{a_3,a_2,a_1,a_0}(\beta)$ durch 3 teilbar ist. Es soll also für jede Belegung β genau dann $\hat{\beta}(\varphi) = 1$ gelten, wenn die Zahl $\text{number}_{a_3,a_2,a_1,a_0}(\beta)$ ein Vielfaches von 3 ist.

Tipp: Bestimmen Sie ein φ in disjunktiver Normalform.

Übung 4.2 Konjunktive Normalform bestimmen, mittel

Entwickeln Sie eine aussagenlogische Formel φ, die angibt, ob die Zahl $\text{number}_{a_3,a_2,a_1,a_0}(\beta)$ größer als 2 ist. Es soll also für jede Belegung β genau dann $\hat{\beta}(\varphi) = 1$ gelten, wenn gerade gilt $\text{number}_{a_3,a_2,a_1,a_0}(\beta) > 2$.

Wandeln Sie dann, falls nötig, φ so um, so dass es in konjunktiver Normalform ist.

Übung 4.3 Addition durch Formeln beschreiben, mittel

Entwickeln Sie vier aussagenlogische Formeln φ_0, φ_1, φ_2 und φ_3 in disjunktiver Normalform, die die Zahl $\text{number}_{a_2,a_1,a_0}(\beta) + 1$ beschreiben. Dabei soll $\hat{\beta}(\varphi_0)$ das niederwertigste Bit angeben, $\hat{\beta}(\varphi_1)$ das zweitniederwertigste Bit usw. Es soll also für jede Belegung β gelten:

$$\text{number}_{a_2,a_1,a_0}(\beta) + 1 = \sum_{i=0}^{3} \hat{\beta}(\varphi_i) \cdot 2^i.$$

Übung 4.4 Normalform bestimmen, schwer

Bestimmen Sie die disjunktive Normalform folgender Formel:

$$(a_1 \lor b_1) \land (a_2 \lor b_2) \land \dots \land (a_n \lor b_n).$$

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

Prüfungsfrage 4.5

16 min

→ Lösung

Normalform bestimmen

Geben Sie zu jeder der folgenden Formeln eine äquivalente Formel in disjunktiver Normalform und eine in konjunktiver Normalform an. Geben Sie explizit an, welche Ihrer Formeln jeweils die disjunktive und welche die konjunktive Normalform ist.

1. $a \land b \land c$
2. $\neg a \land (a \to c)$
3. $(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)$

Prüfungsfrage 4.6

13 min

→ Lösung

Wie Prüfungsfrage 4.5, aber für:

1. $\neg(a \to b) \lor (\neg a \land c)$
2. $(b \leftrightarrow a) \land (b \lor a)$

Prüfungsfrage 4.7

13 min

→ Lösung

Wie Prüfungsfrage 4.5, aber für:

1. $(\neg a \lor b) \to (a \land b)$
2. $(a \lor c) \land (a \to \neg b)$

Prüfungsfrage 4.8

10 min

Zahlen vergleichen

Entwickeln Sie eine aussagenlogische Formel φ, die angibt, ob die Zahl $\text{number}_{a_2,a_1,a_0}(\beta)$ größer oder gleich $\text{number}_{b_2,b_1,b_0}(\beta)$ ist.

(Für eine Variablenbelegung $\beta \colon \{a_0, a_1, a_2, b_0, b_1, b_2\} \to \{0,1\}$ soll also genau dann $\hat{\beta}(\varphi) = 1$ gelten, wenn $\text{number}_{a_2,a_1,a_0}(\beta) \geq \text{number}_{b_2,b_1,b_0}(\beta)$ gilt.)

Prüfungsfrage 4.9

10 min

Spezielle Normalformen

Eine aussagenlogische Formel ist in *2-konjunktiver Normalform*, wenn sie in konjunktiver Normalform ist und jeder Oder-Block höchstens zwei Literale enthält. Beispielsweise ist $(\neg x \lor y) \land z$ in 2-konjunktiver Normalform, die Formel $(x \lor y \lor z) \land \neg y$ jedoch nicht.

Geben Sie eine aussagenlogische Formel an, die zu keiner Formel in 2-konjunktiver Normalform äquivalent ist.

Lösung zu 4.5

1. DNF: $a \land b \land c$
   KNF: $a \land b \land c$
2. DNF: $\neg a$
   KNF: $\neg a$
3. DNF: $(x \land \neg y) \lor (x \land z) \lor (y \land \neg x) \lor (y \land z) \lor (\neg z \land \neg x) \lor (\neg z \lor \neg y)$
   KNF: $(x \lor y \lor \neg z) \land (\neg x \lor \neg y \lor z)$

Lösung zu 4.6

1. DNF: $(a \land \neg b) \lor (\neg a \land c)$
   KNF: $(a \lor c) \land (\neg a \lor \neg b) \land (\neg b \lor c)$
2. DNF: $a \land b$
   KNF: $a \land b$

Lösung zu 4.7

1. DNF: $(a \land \neg b) \lor (a \land b)$
   KNF: $(a \lor b) \land (a \lor \neg b)$
2. DNF: $(a \land \neg b) \lor (\neg a \land c) \lor (\neg b \land c)$
   KNF: $(a \lor c) \land (\neg a \lor \neg b)$

Teil III

Beweissysteme

Der Film *Twelve Angry Men* eröffnet damit, dass sich die Geschworenen eines Mordprozess in einen Beratungsraum zurückziehen, in dem dann auch der gesamte Film spielen wird. Der Fall ist völlig klar: Der Angeklagte hatte zugegeben, Streit mit dem Opfer gehabt zu haben, er wurde von einer Zeugin dabei gesehen, wie er das Opfer niederstach, ein zweiter Zeuge hat den Angeklagten nach dem Mord aus dem Zimmer des Opfers stürmen sehen und schließlich wurde als Tatwaffe noch das Messer des Angeklagten sichergestellt. Es ist heiß in dem Beratungsraum, obwohl der Film schwarzweiß gedreht ist kann man die schwüle Hitze selbst noch als Zuschauer spüren. Man sympathisiert mit den Elf der Geschworenen, die den Angeklagten schnell schuldig sprechen wollen, um so der klaustrophobischen Atmosphäre des Raumes zu entrinnen.

Nur einer der Herren möchte wenigstens über den Fall reden, was zu wütenden Erwiderungen führt. Da gäbe es nichts zu reden, die Sache sei völlig klar. Da aber Geschworene einstimmig ihr Urteil fällen müssen, beginnt nun ein rhetorischer Schlagabtausch, in dem der Zweifler von der Schuld des Angeklagten überzeugt werden soll. Nach und nach stellt sich aber – rein durch Diskussionen und Überlegungen – heraus, dass die angeblich so unumstößlichen Fakten auf eher sandigem Boden stehen. Einer nach dem anderen der Twelve Angry Men muss schließlich sein Urteil revidieren, der Angeklagte wird freigesprochen. Der *Beweis der Schuld* konnte nicht erbracht werden, obwohl er doch so klar schien.

Auch in der Mathematik und besonders in der Logik ist ein *Beweis* letztendlich immer ein *Überzeugungsversuch*. Wenn Sie eine Behauptung *beweisen* wollen, so müssen Sie *Zweifler* überzeugen. Diese Zweifler können sich als sehr störrisch erweisen, im schlimmsten Fall müssen Sie jeden Argumentationsschritt haarklein begründen. Der Zweifler ist Ihr Gegenspieler, wenn Sie einen Beweis aufschreiben. Ständig fragt er nach »Wieso sollte das so sein?« oder kürzer »Warum?«, er ähnelt dabei ein wenig einem Kleinkind, dass sich die Welt in einer endlosen Kette von »Warum?«-Fragen von seinen Eltern erklären lässt (und diese damit langsam aber sicher in die Verzweiflung treibt).

Damit Sie bei einem Beweis überhaupt eine Chance haben, einen hartnäckigen Zweifler zu überzeugen, muss es irgendwelche Argumente geben, die er akzeptiert. Ein *Beweissystem* legt solche »von beiden Seiten anerkannte« Argumente fest. Beispielsweise gibt es im Beweissystem von Hilbert *Axiome*, die man in einem Beweis ohne weitere Begründung immer benutzen darf. Wenn Ihr Zweifler an der Richtigkeit selbst dieser Axiome zweifelt, dann können Sie im ruhigen Gewissens empfehlen, sich doch bitte an seine Eltern zu wenden oder sich am besten gleich in ein Logikwölkchen aufzulösen.

5-1

Kapitel 5
Beweise: Eine Einführung
Die Maschinensprache der Mathematik

5-2

Lernziele dieses Kapitels

1. Unterschied zwischen formalen und normalen Beweisen kennen
2. Begriffe der Korrektheit und der Vollständigkeit kennen
3. Struktur eines normalen Beweises nachvollziehen können

Inhalte dieses Kapitels

Worum es heute geht

Anfang des letzten Jahrhunderts war es dann soweit: Die Mathematiker hatten in Form der Mengenlehre und der Typlehre endlich ein Fundament, auf dem sich die gesamte Mathematik mit all ihren Teilzweigen aufbauen lassen konnte. Alles konnte immer weiter zurückgeführt werden bis auf einige grundlegende, zweifelsohne wahre Aussagen. Die Mathematiker Whitehead und Russel machten sich daran, in ihrem epochalen Werk *Principia Mathematica* aufzuschreiben, wie dies geht. Von der Reduktion auf das Fundament der Mengenlehre wurden selbst die Zahlen nicht verschont, so dass der mathematische Sachverhalt »$1+1=2$« dann auch erst nach über *hundert Seiten* bewiesen wird.

An dieser Stelle fragt sich selbst der gegenüber Formalismen aufgeschlossene Leser besorgt, ob hier nicht gegen das gesetzliche Gebot der Verhältnismäßigkeit verstoßen wird und zumindest ein kleines Ordnungsgeld angebracht erscheint, um solchen formalistischen Auswüchsen Einhalt zu gebieten. Warum brauchen einige der größten Mathematiker ihrer Zeit hunderte Seiten, um Rechenaufgaben aus der Vorschule zu beweisen?

Der Grund ist letztlich der, dass Mathematiker immer in panischer Angst davor leben, dass eine ihrer Behauptungen falsch sein könnte. Wenn man neue mathematische Sätze beweist, dann benutzt man in aller Regel schon als korrekt erkannte Sätze, die meist auf noch ältere Sätze zurückgehen. Wäre einer der Sätze »weit unten« falsch, so würden die ganzen darauf errichteten mathematischen Satzgebäude wie ein Kartenhaus in sich zusammenfallen. (Sie erinnern sich vielleicht noch and die Vorlesung über die Semantik der Aussagenlogik: »Aus einer falschen Prämissen kann man alles folgern.«) Deshalb gilt es unter allen Umständen zu verhindern, dass sich auch nur der kleinste Fehler einschleicht.

Selbst wirklich kleine Ungenauigkeiten können weitreichende Konsequenzen haben. In späteren Veranstaltungen werden Sie noch das so genannte P-NP-Problem kennen lernen, das wohl berühmteste ungelöste Problem der Theoretischen Informatik. Da für die Lösung dieses Problems \$1.000.000 Belohnung durch das Cray-Institut ausgesetzt wurden, wundert es nicht, dass häufig Leute behaupten, einen Beweis für $\text{P} = \text{NP}$ gefunden zu haben. Diese

Beweise, wenn sie nicht völlig abwegig erscheinen, werden dann von verschiedenen Theoretikern überprüft im Rahmen eines so genannten Peer-Reviews. Ich selbst hatten schon das Vergnügen, mehrere solcher Beweise auf dem Schreibtisch zu haben. Bei einem davon (allerdings für eine etwas schwächere, dennoch aber auch bahnbrechende Aussage) war der Beweis schon von anderen Leuten grob überprüft worden und es waren zunächst keine Fehler entdeckt worden.

Es hat zwei Tage harte Arbeit gekostet, sich in die recht komplexen Überlegungen einzuarbeiten, es wurden auch Ideen aus verschiedensten Teilgebieten der Mathematik genutzt (von denen ich zum Teil nur, höflich formuliert, rudimentäre Kenntnisse hatte). In einem so umfangreichen Beweis (zwölf Seiten in der kurzen Fassung) ist es sehr üblich, um nicht zu sagen notwendig, einige Details wegzulassen. So gab es etwa in der Mitte der Beweises eine umfangreiche Fallunterscheidung, bei der einige Fälle weggelassen wurden, die analog zu den anderen funktionierten. So jedenfalls dachte der Autor des Beweises und ich sah das zunächst genauso. Wenn nun aber ein Satz wirklich monumentale Auswirkungen hätte, dann wird man als Leser auch mal hyperkritisch. Beim dritten Lesen beginnt man dann auch, die weggelassenen Fallunterscheidungen doch im Kopf durchzugehen. Dabei stellte sich dann heraus, dass merkwürdigerweise bei einem dieser Unterpunkte ein Vorzeichen anders hätte sein müssen als bei den anderen. Mit diesem falschen Vorzeichen löste sich dann aber nach und nach der ganze Beweis auf, da alles, was nun folgte, nicht mehr stimmte.

Mathematiker haben in den letzten Jahrtausenden immer wieder die Erfahrung gemacht, dass scheinbar *sehr* überzeugende Argumente falsch sein können. Sogar Beweise können überzeugend, aber falsch sein. Deshalb hat man schon früh begonnen, sich über *formale Beweise* Gedanken zu machen. Das sind Beweise, die so strengen Regeln folgen, dass sie prinzipiell sogar von einem Computer überprüft werden können. Gibt es einen formalen Beweis für eine Aussage, so kann man sich das mühselige Fehlersuchen sparen – die Aussage ist dann einfach wahr. Punkt. Ende der Diskussion. (An dieser Stelle fangen dann übrigens in Form des zweiten Gödel'schen Unvollständigkeitssatzes die Diskussionen erst richtig an, aber das wird für Ihr Studium glücklicherweise vollkommen unwichtig sein.)

Es wird Sie freuen zu erfahren, dass $1 + 1 = 2$ mittlerweile formal bewiesen wurde, also zu den unumstößlichen Weisheiten der Mathematik gehört. Wobei näturlich der Gödel'sche Unvollständigkeitssatz zu beachten ist…

5.1 Was sind Beweise?

5.1.1 Motivation

Kleine Geschichte des Beweises in der Justiz. 5-4

Um die *Schuld* eines Angeklagten *zu beweisen,* hat man verschiedene Verfahren genutzt:

- Die Schuld war bewiesen, wenn der Angeklagte *in einem Kampf unterlegen war*.
- Später war die Schuld erst bewiesen, wenn der Angeklagte *gestanden* hatte. (Deshalb musste man ihn foltern.)
- Heute ist die Schuld bewiesen, wenn ein *Richter durch Argumente überzeugt wird*.

Beweise durch Besiegte sind keine guten Beweise. 5-5

Artist: Albrecht Dürer, public domain

Unknown author, public domain

5-6 Beweise unter Folter sind keine guten Beweise.

5.1.2 Mathematische Beweise

5-7 **Zur Geschichte des Beweises in der Mathematik.**
Die *antiken Mathematiker* wie zum Beispiel Euklid haben bereits *recht moderne Beweise geführt*. Im späten Mittelalter wurde *weniger streng bewiesen*. (Eine Rechnung von Euler würde man Ihnen heute nicht mehr durchgehen lassen.) Die Idee des *formalen, strengen Beweises* bildet sich Ende des 19. Jahrhunderts. Hier waren zum Beispiel Cantor, Gödel und Hilbert wichtig.

5-8 **Was ist nun ein mathematischer Beweis?**
Ein *mathematischer Beweis* soll einen *Menschen* davon *überzeugen*, dass eine *Behauptung wahr ist*. Der Beweis ist ein *Text*, der aus einzelnen *Schritten* besteht, die die Behauptung immer mehr untermauern. Wie *detailliert* die Schritte sind, hängt von *der Vorbildung und der Skepsis des Lesers ab*.

5-9 **Ein Dialog zwischen Achilles und der Schildkröte.**
Der Dialog findet zwischen dem großen Helden Achilles und einer Schildkröte statt.[1] Die Schildkröte berichtet Achilles von ihrer neuesten Entdeckung: Zu jeder Formel gibt es eine äquivalente Formel in DNF. Achilles ist nicht überzeugt und muss nun von der Schildkröte überzeugt werden.

Achilles Guten Tag Herr Schildkröte!

Schildkröte Hallo Achilles! Wie geht es Ihnen?

Achilles Danke gut. Was gibt es Neues bei Ihnen?

Schildkröte Oh! Ich habe etwas Interessantes herausgefunden: Zu jeder ausssagenlogischen Formel φ gibt es eine äquivalente Formel φ' in disjunktiver Normalform.

Achilles Was Sie nicht sagen! Sind Sie sich da sicher?

Schildkröte Hundertprozentig.

Achilles Das ist wirklich erstaunlich; ich kann es gar nicht glauben. Sie müssen mich erstmal davon überzeugen.

Schildkröte Gerne. Wieso glauben Sie denn nicht an meine Entdeckung?

Achilles Nun, ich könnte mir vorstellen, dass es doch Formeln gibt, für die sie nicht zutrifft.

Schildkröte Gut, nehmen wir doch mal eine beliebige Formel her. Nennen wir sie φ, einverstanden?

Achilles Wenn Sie es wünschen.

Schildkröte Sei also φ eine beliebige Formel. Dann kommen in φ nur endlich viele Variablen vor.

Achilles Ja, natürlich, die Formel ist ja nur endlich lang.

Schildkröte Genau, sehr richtig. Nun stellen wir eine Wahrheitstafel für die Formel auf.

Achilles Ich erinnere mich noch dunkel, wie dies geht.

Schildkröte In dieser Wahrheitstafel gibt es einige Zeilen, bei denen die Formel zu 1 auswertet. Zu jeder *dieser* Zeilen bilden wir ein Monom. Die Formel φ' ist dann die Veroderung dieser Monome.

Achilles Das ging etwas schnell, aber ich denke, ich kann Ihnen noch folgen. Ich sehe jetzt, wie Sie die Formel φ' bilden. Aber wieso ist diese nun in disjunktiver Normalform und warum ist sie äquivalent zu φ?

Schildkröte Nun, dass die Formel in disjunktiver Normalform ist, sollte Ihnen eigentlich klar sein.

Achilles Jetzt, wo Sie es sagen …

Schildkröte Ich muss Sie nun noch überzeugen, dass φ' äquivalent zu φ ist. Leider rennt mir die Zeit davon, weshalb ich dies gerne bei einem anderen Treffen erklären würde.

[1] Wer mehr über Achilles und die Schildkröte erfahren möchte, dem sei das Buch »Gödel, Escher, Bach« von Douglas Hofstadter empfohlen.

Achilles Oh, kein Problem. Bis dahin kann ich ja mal selbst über diesen Beweisteil nachdenken.

Merke
Ein *mathematischer Beweis* ist der »Text der Schildkröte«.

Wie überzeugend Mathematiker Beweise finden. 5-10

Im Handbuch des Beamer-Pakets, mit dem die Texte zu dieser Veranstaltung erstellt worden sind, gibt es als Beispieltext einen sehr knappen Beweis. Etwa einmal pro Quartal erhalte ich eine E-Mail, in der sich jemand über den Beweis beschwert. Ein netter Mensch aus Darmstadt schreibt:

```
... Sehr irritiert hat nicht allerdings der "Beweis" im Manual,
dass es keine grösste Primzahl gibt und ich möchte Sie hiermit
bitten ihn nochmals zu überarbeiten. Denn naiv wie ist glaubt
man nach dem Studium des Manuals tatsächlich, dass der Beweis
stimmt ...
```

Ein anderer Nutzer aus Wien schreibt:

```
... Ich kann es mir zwar nicht ganz vorstellen, aber sofern es
wirklich noch niemandem aufgefallen ist: die Version von Euklids
Beweis in der Beamer Doku/Templates ist falsch ...
```

Hier noch eine Meinung aus New Jersey:

```
... I am aware that you get a lot of unsolicited email regarding
beamer, but I hope that you will appreciate a minor correction in
the example that is used throughout the user guide ...
```

Formale versus normale mathematische Beweise. 5-11

Der normale mathematische Beweis

- Ein *normaler Beweis* besteht aus *textuell beschriebenen Beweisschritten*.
- Die Korrektheit wird *von Menschen überprüft*.
- Über die Korrektheit *ist man sich nicht immer gleich einig*.

Der formale mathematische Beweis

- Ein *formaler Beweis* besteht aus *standardisierten, extrem einfachen Beweisschritten*.
- Sie sind *so einfach*, dass sie *leicht automatisch (von einem Programm) überprüft werden können*.
- Über die Korrektheit sollte es *keine Diskussion geben können*.

Zwei Vergleiche. 5-12

Normale mathematische Beweise
$\triangleq$
Beschreibungen von Algorithmen

Formale mathematische Beweise
$\triangleq$
Maschinensprache

5.2 Beweissysteme

5.2.1 Idee

5-13

Was sind Beweissysteme?

Beweissysteme allgemein

Ein *Beweissystem* ist ein System, um *formale Beweise* aufzuschreiben. Das Beweissystem legt *Regeln* fest, wie Beweise aufgebaut sein dürfen. Die Einhaltung der Regeln muss *sehr einfach* zu überprüfen sein. Ein Beweissystem sagt *nicht*, wie man einen Beweis findet, sondern nur, *welche Beweise erlaubt sind*.

Beweissysteme der Aussagenlogik

Beweissysteme der Aussagenlogik regeln, wie Beweise dafür aussehen, dass *Formeln Tautologien sind*.

5.2.2 Beispiele

5-14

Erstes Beweissystem: Wahrheitstafeln

Problemstellung

Wir wollen beweisen, dass eine Formel eine Tautologie ist.

Das Beweissystem »Wahrheitstafel«

In diesem System sind *Beweise* gerade *Wahrheitstafeln*. Genauer ist *ein Beweis dafür, dass φ eine Tautologie ist*, einfach die Wahrheitstafel von φ. Es ist in der Tat einfach, zu überprüfen, ob

1. die Ergebnisspalte konstant 1 ist und
2. alle Einträge der Ergebnisspalte korrekt sind.

5-15

Ein Beweis im Beweissystem »Wahrheitstafel«.

Behauptung
Die Formel $(a \wedge b) \vee (\neg a \wedge b) \vee \neg b$ ist eine Tautologie.

(Formaler) Beweis.

$\beta(a)$	$\beta(b)$	$\hat\beta\big((a \wedge b) \vee (\neg a \wedge b) \vee \neg b\big)$
0	0	1
0	1	1
1	0	1
1	1	1

✎ Zur Diskussion

Welche Nachteile hat das Beweissystem »Wahrheitstafel«?

5-16

Weitere Beweissysteme

Das Beweissystem »Resolution«

In diesem System sind *Beweise* gerade *Folgen von äquivalenten Formeln in KNF*. Welche Folgen erlaubt sind, kommt im Kapitel über Resolution.

Das Beweissystem »Hilbertkalkül«

In diesem System sind *Beweise* gerade *Folgen von Tautologien*. Die *letzte Formel* muss gerade die Behauptung sein. Welche Folgen erlaubt sind, kommt im Kapitel über Hilbertkalküle.

5.2.3 Korrektheit und Vollständigkeit

»Gute« Beweissysteme sind »korrekt« und »vollständig«. 5-17

▶ Definition
Ein Beweissystem der Aussagenlogik heißt

1. *korrekt*, wenn sich *nur Tautologien* beweisen lassen, und
2. *vollständig*, wenn sich *alle Tautologien* beweisen lassen.

- Das Wort »korrekt« wird hier in zwei Bedeutungen gebraucht:
  1. Ein *einzelner Beweis* ist korrekt, wenn er gemäß den Regeln des Systems aufgebaut ist.
  2. Ein *Beweissystem* ist korrekt, wenn es korrekte Beweise nur für Tautologien gibt.

▶ Satz
Das Beweissystem »Wahrheitstafeln« ist korrekt und vollständig.

(Ohne Beweis. Argghh…!)

5.3 Anatomie eines natürlichsprachlichen Beweises

5.3.1 Die Behauptung

Ein mathematischer Satz und sein Beweis. 5-18

Satz (Bolzano-Weierstraß)
Jede beschränkte unendliche Folge reeller Zahlen besitzt eine konvergente Teilfolge.

Einen solchen Satz beweist man in drei Schritten:

1. Man macht sich die Behauptung an einem Beispiel und einem Gegenbeispiel klar.
2. Man hat eine *Beweisidee*.
3. Man schreibt den Beweis mittels *Beweisrezepten* und *Schlüsselformulierungen* auf.

In einem Lehrbuch oder einer Vorlesung (auch der heutigen…) bekommt man meist nur den dritten Teil gezeigt.

5.3.2 Der Beweis

Schritt 3: Ein typischer möglicher Beweistext 5-19
»Sei $(x_1,x_2,x_3,\dots)$ eine beschränkte, reelle Folge. Sei $I_1=[a,b]$ ein Intervall mit $x_i \in I_1$ für alle $i \geq 1$. Wir konstruieren eine konvergente Teilfolge $(x_{i_1},x_{i_2},x_{i_3},\dots)$ wie folgt: Sei $i_1=1$. Teile nun I_1 in die zwei Intervalle $I_1'=[a,(a+b)/2]$ und $I_1''=[(a+b)/2,b]$. Dann enthält eines der Intervalle unendlich viele der x_i. Sei I_2 dieses Intervall. Sei i_2 der kleinste Index mit $i_2>i_1$ und $x_{i_2}\in I_2$. Unterteile nun wieder I_2 und sei I_3 eine Hälfte, die unendlich viele Folgenglieder enthält. Sei i_3 minimal, so dass $i_3>i_2$ und $x_{i_3}\in I_3$. Auf diese Art wird die Folge $(x_{i_1},x_{i_2},x_{i_3},\dots)$ gebildet. Dies ist offenbar eine Teilfolge von $(x_1,x_2,x_3,\dots)$ und sie ist konvergent, da sie eine Cauchy-Folge ist.«

5.3.3 Analyse

Analyse verschiedener Formulierungen 5-20
»Sei«

> »Sei $(x_1,x_2,x_3,\dots)$ eine beschränkte, reelle Folge.«

Im Originalsatz heißt es nur »Jede beschränkte unendliche Folge reeller Zahlen besitzt…«
Statt zu schreiben »für das fünfundzwanzigste Element der Folge gilt« wollen wir lieber kurz schreiben »für x_{25} gilt«. Deshalb wird mittels »sei« ein *Name* für die Folge und auch gleich für die Elemente vergeben. Dies ist das Beweisrezept »Namen vergeben«.
Durch »Sei …mit den Eigenschaften aus der Voraussetzung« wird das Beweisrezept »All-Aussage beweisen« benutzt.

5-21 ## Beweisrezept: *Namen für Teile vergeben*

Ziel

Man möchte über die Teile eines Mathe-Dings »reden«.

Rezept

1. Ist das Ding ein Tupel mit einer festen Anzahl Komponenten (wie zum Beispiel eine Grammatik, die immer aus vier Teilen besteht), so schreibt man »Sei $G = (N,T,S,E)$ eine Grammatik...« oder »Sei $G = (V,E)$ ein Graph...«.
2. Ist das Ding ein Tupel mit einer variablen Anzahl Komponenten, so schreibt man »Sei $(x_1,x_2,x_3,\dots,x_n)$ das Tupel...«. Nebenbei hat man mit n auch einen Namen für die Länge des Tupels eingeführt.
3. Ist das Ding eine abzählbare Menge, so schreibt man »Sei $M = \{m_1,m_2,m_3,\dots,m_n\}$« (bei endlichen Mengen) oder »Sei $M = \{m_1,m_2,m_3,\dots\}$« (bei abzählbar unendlichen Mengen).

5-22 ## Beweisrezept: *All-Aussagen beweisen*

Ziel

Es soll gezeigt werden »für alle Dinge, die so und so sind, gilt blah« oder auch »jedes Ding, das so und so ist, hat die Eigenschaft blah«.

Rezept

1. Beginne den Beweis mit »Sei x ein beliebiges Ding, das so und so ist.«
2. Zeige nun, dass x die Eigenschaft blah hat.

Man sollte sich an eine Konvention zur Vergabe von Variablennamen halten. Beispielsweise bezeichnen Buchstaben wie »n« oder »m« oft natürliche Zahlen, φ hingegen wird eher eine Formel oder eine Funktion benennen.

5-23 ## Analyse verschiedener Formulierungen

> »Sei $I_1 = [a,b]$ ein Intervall ...«

An dem »sei« erkennt man, dass hier wieder *abkürzende Namen* für verschiedene Dinge eingeführt werden. Es wird ein Name I_1 für ein Intervall eingeführt. Weiter wird ein Name a für die untere Grenze des Intervals eingeführt und b als Name für die obere Grenze des Intervals.

> »... mit $x_i \in I_1$ für alle $i \geq 1$.«

Hier wird (diesmal *ohne ein »sei«*) ein neues Symbol eingeführt, nämlich i. Der Teilsatz schränkt ein, dass I_1 nicht beliebig sein darf (wie eben noch suggeriert). Vielmehr muss I_1 so groß sein, dass alle x_i darin vorkommen. Solche *nachgestellten Einschränkungen* sind sehr üblich, aber fies. Dass es überhaupt ein I_1 mit dieser Einschränkung gibt, liegt daran, dass die Folge beschränkt ist. *Hier wird erwartet, dass der Leser dies selber merkt und ergänzt.*

5-24 ## Beweisrezept: *Details weglassen*

Ziel

Der Beweis soll kurz und knapp bleiben.

Rezept

1. Man lässt »langweilige« Teile des Beweises weg.
2. Freundlicherweise schreibt stattdessen »Man kann zeigen, dass...« oder auch »Auf den Nachweis, dass ... gilt, wurde verzichtet«.

Vermeiden sollte man »Trivialerweise gilt ...« oder »Offensichtlich gilt ...«, dies reizt den Leser eher zu argumentieren, dass dies doch nicht so trivial ist.

Für Interessierte sind im Folgenden noch einige weitere Kniffe erklärt, die im Beweis benutzt wurden.

»Wir konstruieren eine konvergente Teilfolge $(x_{i_1}, x_{i_2}, x_{i_3}, \dots)$ wie folgt:«

Durch *»wir konstruieren«* wird angedeutet, dass das Beweisrezept »konstruktiver Beweis« benutzt werden wird. Teil 1 des Rezeptes ist die Konstruktion, sie folgt. Teil 2 des Rezeptes ist der Nachweis, dass das konstruierte Ding die gewünschten Eigenschaften hat. Der Beginn von Teil 2 wurde nicht kenntlich gemacht: Er ist bei »Dies ist offenbar«, man muss die Stelle selber entdecken.

Nebenbei werden wieder Namen eingeführt, nämlich i_1, i_2 und so weiter. Die Namen $x_{\dots}$ sind hingegen schon bekannt und werden *nicht* neu eingeführt.

»Dann enthält eines der Intervalle unendlich viele der x_i. Sei I_2 dieses Intervall.«

Im ersten Satz wird etwas behauptet. Der Beweis wird dem Leser überlassen. In »unendlich viele der x_i« wird, streng genommen, die Variable i kurz eingeführt und es wird erwartet, dass man im Kopf ergänzt »mit $i \geq 1$«. Der zweite Satz führt wieder mittels »sei« einen Namen ein, nämlich I_2.

»…sie ist konvergent, da sie eine Cauchy-Folge ist.«

Hier werden zwei Dinge behauptet:

1. »Sie« ist eine Cauchy-Folge.
2. »Sie« ist konvergent.

Die erste Behauptung ist wieder nachgestellt, kommt aber inhaltlich zuerst. Es wird dem Leser überlassen zu zeigen, dass 1. stimmt. Mittels *»da«* wird angedeutet, dass aus 1. auch 2. folgt. Wie immer muss der Leser wissen, warum dies so ist.

Zusammenfassung dieses Kapitels

▶ Beweissysteme 5-25

Ein *formales Beweissystem* legt *sehr einfache Regeln* fest, wie Beweise aufgebaut sein dürfen.

▶ Wichtigste Eigenschaften von formalen Beweissystemen

Vollständigkeit Alle Tautologien lassen sich beweisen.

Korrektheit Nur Tautologien lassen sich beweisen.

▶ Merke

Formale Beweise müssen *Maschinen* überzeugen, *normale* Beweise müssen *Menschen* überzeugen.

Übungen zu diesem Kapitel

Übung 5.1 Tautologien erkennen, schwer

Man kennt kein Beweissystem, in dem sich für jede Formel φ leicht ein Beweis finden lässt, dass φ eine Tautologie ist. Jedoch ist dies möglich, wenn φ in konjunktiver Normalform ist.

Geben Sie ein Beweissystem und ein effizientes Verfahren zum Finden von Beweisen für Tautologien in konjunktiver Normalform an.

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

8 min

Prüfungsfrage 5.2

Trennung der sprachlichen Ebenen

Im folgenden Text wird die Ebene der Logik stellenweise mit der umgangssprachlichen Ebene vermischt. Schreiben Sie den Text neu, ohne logische Symbole zu »missbrauchen«.

> *Eine Menge M ist endlich* $:= \neg\exists X \subsetneq M : |X| = |M|$.
> $\implies \emptyset$ *ist endlich.*

6-1

Kapitel 6
Der Resolutionskalkül

Nie zwei Variablen gleichzeitig auflösen. . .

6-2

Lernziele dieses Kapitels

1. Resolutionskalkül für die Aussagenlogik kennen
2. Resolutionsbeweise führen können
3. Wissen, dass der Resolutionskalkül vollständig ist

Inhalte dieses Kapitels

Worum es heute geht

Neo wird durch den Architekten vor folgende Entscheidung gestellt: Wenn Neo durch die Tür geht, dann kann er seine Lebensabschnittsgefährtin Trinity retten. Wenn Neo nicht durch die Tür geht, dann kann er statt dessen Zion »retten« (in einem sehr rudimentären Sinne, allerdings). Da Neo bei *Logik für Informatiker* gut aufgepasst hat, verblüfft er den Architekten mit der Erkenntnis, dass er, egal was passiert, Trinity *oder* Zion retten kann.

Hier ein etwas weniger phantastisches Beispiel ähnlicher Bauart: Ihr persönlicher Vermögensverwalter erklärt Ihnen, dass Sie, wenn Sie jetzt anfangen, für das Alter zu sparen, dann haben Sie im Alter mehr Geld. Auf Nachfrage räumt er dann ein, dass Sie, wenn Sie jetzt nicht anfangen, für das Alter zu sparen, natürlich jetzt mehr Geld haben. Das ist schön, denn immer wenn Sie glauben, Sie hätten zu wenig Geld, so können Sie sich mit einer logischen Folgerung trösten: Egal was passiert, Sie haben jetzt mehr Geld oder im Alter mehr Geld!

Schließlich noch ein Beispiel aus der Technischen Informatik: In einer aufwendigen Untersuchung hat das Forscherteam um Professor Black herausgefunden, dass ein kleiner schwarzer Kasten folgende Eigenschaft hat: Wenn an Pin 1 Strom angelegt ist, dann leuchtet LED 1; wird hingegen kein Strom angelegt, so leuchtet LED 2. In Rahmen einer Forschungskooperation mit der Theoretischen Informatik hat sich daraufhin herausgestellt, dass man Kraft logischer Schlüsse hieraus folgern kann, dass immer LED 1 oder 2 leuchtet!

Der logischer Gehalt der Folgerungen von Neo, Ihres Vermögensverwalters oder Professor Blacks ist jedes Mal gleich dürftig: Wenn $(a \to b) \wedge (\neg a \to c)$ gilt, dann gilt $b \vee c$. Diese eigentlich nicht sonderlich aufregende Erkenntnis hat jedoch einen besonderen Namen: man nennt sie die *Resolutionsregel*. Sie beschreibt gewissermaßen, was gelten muss »komme was will«. Egal ob Neo durch die Tür geht, egal ob Sie Geld fürs Alter sparen, egal ob Strom anliegt, bestimmte Dinge passieren auf jeden Fall. Es kann dann sein, dass deshalb wieder andere Dinge auf jeden Fall passieren müssen, die wieder andere Dinge nach sich ziehen. Die Resolutionsregel kann man mehrfach anwenden, um herauszufinden, was alles aus einer Menge von Voraussetzungen folgt.

Das wäre alles nicht weiter der Rede wert (es gibt noch viele andere, ähnliche Regeln, die man prinzipiell immer wieder anwenden kann), wenn die Resolutionsregel nicht eine besondere Eigenschaft hätte: Wie wir sehen werden, lässt sich bei *jeder* kontradiktorischen Formel durch wiederholte Anwendung der Resolutionsregel der innere Widerspruch der Formel irgendwann aufdecken. Daraus kann man im wahrsten Sinne des Wortes »im Handumdrehen« ein Beweissystem basteln, da $\neg\varphi$ genau dann kontradiktorisch ist, wenn φ tautologisch ist.

Wem dieser mathematische Taschenspielertrick zu schnell ging, für den hier das Beweissystem »Resolution« für den Hausgebrauch in einem Satz: »Um zu zeigen, dass φ tautologisch ist, schreibe $\neg\varphi$ in konjunktiver Normalform und wende die Resolutionsregel so lange an, bis ein Widerspruch entsteht.«

6.1 Resolution

6.1.1 Ziel: Ein Beweissystem

6-4 #### Wiederholung: Was waren Beweissysteme?

Beweissysteme allgemein

Ein *Beweissystem* ist ein System, um *formale Beweise* aufzuschreiben. Das Beweissystem legt *Regeln* fest, wie Beweise aufgebaut sein dürfen. Die Einhaltung der Regeln muss *sehr einfach* zu überprüfen sein. Ein Beweissystem sagt *nicht*, wie man einen Beweis findet, sondern nur, *welche Beweise erlaubt sind*.

Beweissysteme der Aussagenlogik

Beweissysteme der Aussagenlogik regeln, wie Beweise dafür aussehen, dass *Formeln Tautologien sind*.

6-5 #### Das Beweissystem Resolution

Problemstellung

Wir wollen beweisen, dass eine Formel in DNF eine Tautologie ist.

Das Beweissystem »Resolution«

In diesem System sind *Beweise* gerade *Folgen von äquivalenten Formeln in* KNF. Welche Folgen erlaubt sind, kommt gleich.

6.1.2 Vorbereitungen

6-6 #### Vorbereitung I: Beweis von Kontradiktionen statt Tautologien.

Wir wollen zeigen, dass eine Formel φ in DNF eine *Tautologie* ist. Das ist genau dann der Fall, wenn $\neg\varphi$ eine *Kontradiktion* ist. Die Formel $\neg\varphi$ lässt sich leicht in eine KNF umwandeln (zweimal De Morgan'sche Regel).
Bei der *Resolution* versucht man zu zeigen, dass eine *Formel in* KNF *eine Kontradiktion ist*.

6-7 #### Vorbereitung II: Die Resolutionsregel.

▶ Satz: Resolutionsregel
Für alle Formeln φ und φ' gilt:

$$(\varphi \vee a) \wedge (\varphi' \vee \neg a) \equiv (\varphi \vee a) \wedge (\varphi' \vee \neg a) \wedge (\varphi \vee \varphi')$$

Beweis. Zum Beispiel durch eine Wahrheitstafel.[1] □

Kommentare zum Beweis

[1] Zur Erinnerung: Ein »normaler« Beweis wie dieser ist ein »Überzeugungsversuch«. Es geht darum, Sie als Leser von der Richtigkeit der Aussage zu überzeugen. – Und, ist dies gelungen?

6-8 #### Wie sehen Resolutionsbeweise aus?

Ein Resolutionsbeweis ist eine *Folge von äquivalenten Formeln in* KNF. Jede Formel geht aus der vorherigen durch eine der folgenden beiden Operationen hervor:

1. Äquivalente Umformung einer der Klauseln (also Ausnutzung der Kommutativität oder Entfernung eines doppelten Literals).
2. Anwendung der Resolutionsregel auf zwei Klauseln. Dadurch entsteht eine neue Klausel, die hinten angefügt wird.

Die letzte Formel im Beweis muss die »leere« Klausel `f` enthalten. Diese leere Klausel entsteht, wenn man die Resolutionsregel auf die Klauseln a und $\neg a$ anwendet (φ und φ' sind leer).

Ein Beweis im Beweissystem »Resolution«. 6-9

Behauptung
Die Formel $(c \wedge b) \vee (c \wedge \neg b) \vee (\neg a \wedge \neg c) \vee (a \wedge \neg c)$ ist eine Tautologie.

Beweis.
Die Formel $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (a \vee c) \wedge (\neg a \vee c)$ ist eine Kontradiktion:

1. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (a \vee c) \wedge (\neg a \vee c)$
2. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (\neg a \vee c)$
3. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a)$
4. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a) \wedge (\neg c \vee \neg c)$
5. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a) \wedge \neg c$
6. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a) \wedge \neg c \wedge (c \vee c)$
7. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a) \wedge \neg c \wedge c$
8. $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (c \vee a) \wedge (c \vee \neg a) \wedge \neg c \wedge c \wedge \mathtt{f}$

6.1.3 Graphische Schreibweise

Verbesserung der Schreibweise. 6-11

Probleme mit der Schreibweise

Es ist unschön, dass wir die Literale in den Klauseln umstellen müssen und Duplikate entfernen müssen. Ebenso ist es unschön, dass wir dieselben Klauseln immer wieder hinschreiben müssen.

Lösungen der Probleme

- Statt der Klauseln schreiben wir nur die *Mengen der in den Klauseln vorkommenden Literale auf*.

Die »echte« Klausel (eine Zeichenkette)	Mengenschreibweise
$(a \vee \neg a')$	$\{a, \neg a'\}$
$(\neg a' \vee a)$	$\{a, \neg a'\}$
$(a \vee b \vee c \vee a \vee \neg b)$	$\{a, b, \neg b, c\}$
$(\neg a)$	$\{\neg a\}$
$\mathtt{f}$	$\emptyset$

- Statt der ganzen Formel schreiben wir immer nur die neue Klausel auf.

Neue Schreibweise für den Beweis. 6-12

Behauptung
Die Formel $(c \wedge b) \vee (c \wedge \neg b) \vee (\neg a \wedge \neg c) \vee (a \wedge \neg c)$ ist eine Tautologie.

Beweis.
Die Formel $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (a \vee c) \wedge (\neg a \vee c)$ ist eine Kontradiktion:

1. $\{\neg c, \neg b\}$, $\{\neg c, b\}$, $\{a, c\}$, $\{\neg a, c\}$
2. $\{\neg c\}$
3. $\{c\}$
4. $\emptyset$

Beweis (graphische Darstellung).
Die Formel $(\neg c \vee \neg b) \wedge (\neg c \vee b) \wedge (a \vee c) \wedge (\neg a \vee c)$ ist eine Kontradiktion:

$$\begin{tikzcd}[column sep=small]
\{\neg c, \neg b\} \arrow[dr, no head] & & \{\neg c, b\} \arrow[dl, no head] & & \{a, c\} \arrow[dr, no head] & & \{\neg a, c\} \arrow[dl, no head] \\
& \{\neg c\} \arrow[drr, no head] & & & & \{c\} \arrow[dll, no head] & \\
& & & \emptyset & & &
\end{tikzcd}$$

✎ Zur Übung 6-13

Geben Sie einen Resolutionsbeweis dafür an, dass folgende Formel eine Kontradiktion ist:

$$(\neg a \vee \neg b \vee c) \wedge (a \vee \neg c) \wedge (b \vee c) \wedge (\neg a \vee \neg c) \wedge (a \vee \neg b)$$

6.2 Korrektheit und Vollständigkeit

6.2.1 Korrektheit

6-14 Der Resolutionskalkül ist korrekt.

▶ Satz
Der Resolutionskalkül ist korrekt.

Beweis. Sei φ eine Formel in DNF und P ein Resolutionsbeweis für φ. Dies bedeutet:

- Die letzte Formel im Beweis P ist eine Kontradiktion (sie enthält schließlich die Klausel `f`).
- Alle Formeln im Beweis P sind äquivalent.
- Die erste Formel im Beweis P ist die Negation von φ.

Also ist auch die Negation von φ eine Kontradiktion und somit ist φ eine Tautologie. □

Man beachte: Der Begriff »Beweis« wird hier mal wieder auf zwei Ebenen verwendet.

6.2.2 Vollständigkeitssatz

6-15 Der Resolutionskalkül ist vollständig.

▶ Satz
Der Resolutionskalkül ist vollständig.

Genauer bedeutet dies: Ist eine beliebige Tautologie φ gegeben und wandelt man $\neg\varphi$ in eine KNF um, so gibt es einen Resolutionsbeweis, dass dies eine Kontradiktion ist.

6.2.3 *Beweis der Vollständigkeit

6-16 Beweisrezept: *Induktion*

Ziel
Es soll gezeigt werden, dass eine Behauptung B für alle $n \in \{1,2,3,\dots\}$ gilt.

Rezept

1. Zeige, dass die Behauptung B für $n = 1$ gilt.
   (Tipp: Hier kann man probieren, einfach »trivial« zu schreiben; das wird oft akzeptiert.)
2. Man nimmt an, dass B für ein vorgegebenes n gilt (aber vielleicht nicht für andere n). Man folgere, dass B dann zumindest auch für $n+1$ gilt.

6-17 Beweis des Vollständigkeitssatzes.
Zunächst nochmal die zu beweisende Behauptung:

> *Zu jeder kontradiktorischen Formel ψ in konjunktiver Normalform gibt es einen Resolutionsbeweis, dass dies eine Kontradiktion ist.*

Beweis. Wir beweisen die Behauptung durch eine Induktion über die *Anzahl n der in ψ vorkommenden unterschiedlichen Variablen.*[1]
Sei $n = 1$. Wir müssen zeigen, dass für jede Kontradiktion in KNF, in der nur eine Variable vorkommt, ein Resolutionsbeweis existiert.[2] Die einzige Kontradiktion in KNF mit nur einer Variablen v lautet in Klauseldarstellung $\{v\}, \{\neg v\}$. Hier kann aber in einem Schritt die Klausel `f` abgeleitet werden und wir sind fertig.
Für den Induktionsschritt nehmen wir an, für *alle Kontradiktionen in KNF mit n Variablen gäbe es einen Resolutionsbeweis*. Sei nun eine beliebige kontradiktorische KNF ψ mit $n+1$ Variablen gegeben.[3]
Unser Ziel ist es zu zeigen, dass es für ψ einen Resolutionsbeweis gibt. Wir wollen also einen *Existenzbeweis* führen.[4] Im Folgenden geben wir zunächst an, wie der Resolutionsbeweis aussehen soll; dann zeigen wir, dass es wirklich einer ist.[5]

Kommentare zum Beweis

[1] Hinweis auf das Beweisrezept und darauf, worüber überhaupt die Induktion läuft.

[2] Einfach zu zeigen, »trivial« würde (mir) aber als Begründung nicht genügen.

[3] Induktionsvoraussetzung

[4] Überdeutlicher Hinweis auf das Beweisrezept. . .

[5] Mal wieder ein »Inhaltsverzeichnis des Beweises«

Zu dem gegebenen ψ wenden wir die Resolutionsregel in einer beliebigen Reihenfolge so lange an, bis keine neuen Klauseln mehr entstehen. Dies liefert eine große KNF, die wir im Folgenden ψ' nennen wollen.[6]
Wir wollen nun zeigen, dass ψ' die Klauseln `f` enthält und somit ein Resolutionsbeweis dafür ist, dass ψ eine Kontradiktion ist.[7]
Beginnen wir damit zu zeigen, dass ψ' die Klausel $\{v\}$ enthält. Dazu bilden wir eine Formel ρ aus ψ' nach folgenden Vorschriften:

1. Streiche alle Klauseln komplett, in denen $\neg v$ vorkommt.
2. Streiche v aus allen Klauseln, in denen es vorkommt.

Nun gilt:[8]

1. Die Formel ρ enthält nur n Variablen[9] und ist ebenfalls eine Kontradiktion (da ein Modell von ρ auch ein Modell von ψ' wäre, belegte man v mit 0).
2. Nach Induktionsvoraussetzung gibt es einen Resolutionsbeweis dafür, dass ρ eine Kontradiktion ist. Seine letzte Formel enthält die leere Klausel $\emptyset$.
3. Da in ψ' alle überhaupt möglichen Resolutionen ausgeführt wurden, sind alle im Resolutionsbeweis von ρ gemachten Schritte auch in ψ' enthalten, nur dass gegebenfalls auch v noch in den Klauseln vorkommt.
4. Da der Resolutionsbeweis von ρ die leere Klausel enthält, enthält also auch ψ' entweder die leere Klausel (und wir sind ganz fertig) oder die Klausel $\{v\}$.

Mit genau demselben Argument wie eben, wobei allerdings statt v immer $\neg v$ geschrieben wird, zeigt man: In ψ' kommt auch $\{\neg v\}$ vor.
Da ψ' nun sowohl die Klauseln $\{v\}$ und $\{\neg v\}$ enthält, enthält es auch $\emptyset$. Damit ist alles gezeigt.[9] $\square$

[6] Das war schon die ganze Konstruktion. Diesmal ist wirklich nicht sofort klar, warum diese Konstruktion die behaupteten Eigenschaften haben soll.

[7] Teil 2 eines Existenzbeweises: Das konstruierte Ding hat die gewünschten Eigenschaften.

[8] Das Folgende macht man sich am besten an einem Beispiel klar.

[9] Wir sind v ja losgeworden.

[9] Das ist doch schön.

Zusammenfassung dieses Kapitels

▶ Der allgemeine Resolutionsschritt 6-18

$$\begin{array}{ccc} A \cup \{v\} & & B \cup \{\neg v\} \\ & \diagdown \quad \diagup & \\ & A \cup B & \end{array}$$

Beispiel

$$\begin{array}{ccc} \{a, \neg b, v\} & & \{\neg b, c, \neg v\} \\ & \diagdown \quad \diagup & \\ & \{a, \neg b, c\} & \end{array}$$

Merke
Man darf nie zwei Variablen gleichzeitig auflösen.

$$\begin{array}{ccc} \{a, v, w\} & & \{\neg b, \neg v, \neg w\} \\ & \diagdown \quad \diagup & \\ & \{a, \neg b\} & \end{array}$$

▶ Der Resolutionskalkül

Der *Resolutionskalkül* ist ein *Beweissystem*, in dem man beweist, dass eine *Formel φ in* DNF *eine Tautologie* ist. Er funktioniert so:

1. Schreibe die Formel $\neg\varphi$ als KNF auf; benutze die Mengenschreibweise für die Klauseln.
2. Wende so lange wie nötig auf zwei geeignete Klauseln die Resolutionsregel an, bis die Klausel $\emptyset$ erreicht ist.

▶ Satz

Die Resolution ist ein vollständiges und korrektes Beweissystem.

Übungen zu diesem Kapitel

Übung 6.1 Einen Resolutionsbeweis führen, leicht

Bauingenieurwesen für Anfänger

Nachdem Ensel und Krete die Hexe in den Ofen gestoßen haben, wollen sie sich über das Knusperhäuschen hermachen. Doch wie allgemein bekannt ist, muss man beim Verspeisen eines solchen Hauses sehr vorsichtig sein, da diese Häuser zur Instabilität neigen. Die beiden wenden sich zunächst einer Wand zu, die aus drei Lebkuchen besteht. Da Ensel erfolgreich Knusperhäuschenarchitektur studiert hat, erkennt er, dass folgende Regeln aus Sicherheitsgründen unbedingt einzuhalten sind.

1. *Von den beiden ersten Lebkuchen darf höchstens einer entfernt werden.*
2. *Wenn man den dritten entfernt, muss man auch den zweiten entfernen.*
3. *Wenn man den zweiten entfernt und den ersten nicht, dann darf man den dritten nicht entfernen.*

Da Krete in Logik aufgepasst hat, weiß sie, dass man vom dritten Lebkuchen besser die Finger lässt. Dies kann man beweisen, indem man die Unerfüllbarkeit der Formel

$$\varphi = (\neg(a_1 \wedge a_2)) \wedge (a_3 \to a_2) \wedge ((\neg a_1 \wedge a_2) \to \neg a_3) \wedge a_3$$

zeigt, worin die Variablen a_1, a_2, a_3 den Aussagen »Der erste, zweite beziehungsweise dritte Lebkuchen darf entfernt werden.« entsprechen.

Bringen Sie dazu die Formel φ mit Hilfe des Algorithmus aus der Vorlesung in konjunktive Normalform. Zeigen Sie dann die Unerfüllbarkeit von φ mit Hilfe des Resolutionskalküls.

(Diese Aufgabe ist dem Buch *Logik für Informatiker* von Martin Kreuzer und Stefan Kühling entnommen.)

Übung 6.2 Einen Resolutionsbeweis führen, leicht

Zeigen Sie mit dem Resolutionskalkül, dass $(a \to b) \vee (a \wedge \neg(b \vee c)) \vee (a \wedge c)$ eine Tautologie ist.

Übung 6.3 Einen Resolutionsbeweis führen, mittel

Zeigen Sie mit dem Resolutionskalkül, dass d aus der Formel $\varphi = (\neg a \to (b \vee c)) \wedge ((c \wedge \neg b) \to a) \wedge (\neg(a \wedge b) \wedge d)$ folgt. (Mit anderen Worten: $\varphi \to d$ ist eine Tautologie.)

Übung 6.4 Einen Existenzbeweis führen, schwer

Wir sagen, eine Formel φ *beschreibt* eine Funktion $f\colon \{0,1\}^n \to \{0,1\}$, wenn Folgendes gilt:

1. In der Formel φ kommen nur Variablen aus der Menge $\{a_1, \dots, a_n\}$ vor.
2. Für alle $x = x_1 \dots x_n \in \{0,1\}^n$ und für alle Variablenbelegungen β gilt: Wenn $\beta(a_i) = x_i$ für alle $i \in \{1, \dots, n\}$, dann $\hat{\beta}(\varphi) = f(x)$.

Beispielsweise wird die Funktion f mit $f(x_1 x_2) = x_1 \cdot x_2$ durch $\varphi = a_1 \wedge a_2$ beschrieben.

Beweisen Sie, dass es für jede Funktion $f\colon \{0,1\}^n \to \{0,1\}$ eine Formel φ gibt, die f beschreibt. Gehen Sie dazu folgendermaßen vor:

1. Machen Sie sich klar, was hier zu beweisen ist, indem Sie sich mehrere konkrete Beispiele für Funktionen f und beschreibende Formeln φ überlegen.
2. Geben Sie ein allgemeines Verfahren an, um aus einer Funktion f eine sie beschreibende Formel φ zu konstruieren.
3. Beweisen Sie, dass das nach Ihrem Verfahren konstruierte φ tatsächlich die Eigenschaften aus obiger Definition besitzt.

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

12 min Prüfungsfrage 6.5 → Lösung

Resolutionsbeweis führen

Zeigen Sie mithilfe des Resolutionskalküls, dass

$$(a \vee b) \wedge (c \vee \neg b) \wedge (c \vee a) \wedge (b \vee \neg a) \wedge (\neg c \vee \neg b)$$

eine Kontradiktion ist.

14 min Prüfungsfrage 6.6 → Lösung

Resolutionsbeweis führen

Wandeln Sie folgende Formel zunächst in KNF um:

$$(b \vee a \vee d) \wedge (\neg a \to \neg d) \wedge (b \leftrightarrow c) \wedge (b \vee \neg a \vee c) \\ \wedge (\neg b \vee a) \wedge (\neg a \vee \neg c)$$

Zeigen Sie dann mithilfe des Resolutionskalküls, dass die Formel eine Kontradiktion ist.

12 min Prüfungsfrage 6.7

Resolutionsbeweis führen

Zeigen Sie mithilfe des Resolutionskalküls, dass

$$(\neg a \wedge \neg b) \vee (\neg d \wedge \neg a \wedge b) \vee (d \wedge \neg a) \vee (a \wedge c \wedge \neg b) \\ \vee (d \wedge \neg a \wedge \neg b) \vee (\neg c \wedge d) \vee (\neg c \wedge \neg b) \vee (a \wedge b)$$

eine Tautologie ist.

12 min Prüfungsfrage 6.8 → Lösung

Einen Beweis im Resolutionskalkül führen

Zeigen Sie mit dem Resolutionskalkül, dass die folgende Formel eine Kontradiktion ist:

$$(\neg a \vee \neg b \vee c) \wedge (a \vee c) \wedge (a \vee b) \wedge (a \vee \neg b) \\ \wedge (\neg a \vee \neg b \vee \neg c) \wedge (\neg a \vee b)$$

Bemerkung: Bei genauem Hinsehen wird man feststellen, dass es sich hier wieder um die Geschichte mit dem Hamster und dem Bären aus Übung 2.9 handelt. Wir zeigen hier, dass die Formel kontradiktorisch ist. Wolf und Hamster haben somit keine Chance, dem Bären einen Kuchen zu backen, der ihm auch schmeckt.

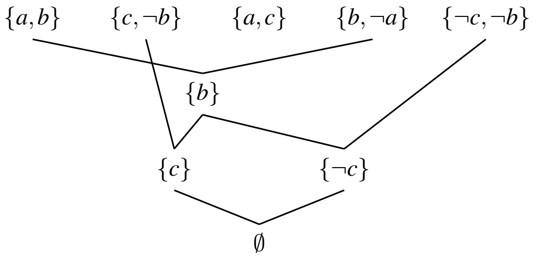
14 min Prüfungsfrage 6.9 → Lösung

Einen Beweis im Resolutionskalkül führen

Zeigen Sie mit dem Resolutionskalkül, dass die folgende Formel eine Tautologie ist:

$$\big(\neg((a \wedge b) \to \neg c)\big) \vee (\neg a \wedge \neg b \wedge \neg c) \vee (\neg a \wedge b \wedge c) \\ \vee (\neg a \wedge b \wedge \neg c) \vee (a \wedge \neg c) \vee (\neg b \wedge c)$$

Lösung zu 6.5

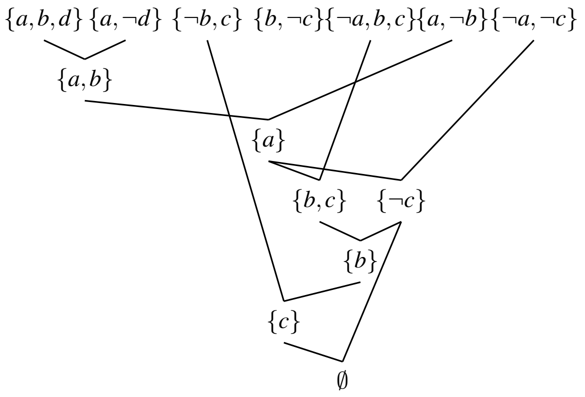


Lösung zu 6.6

Die Formel lautet in KNF:

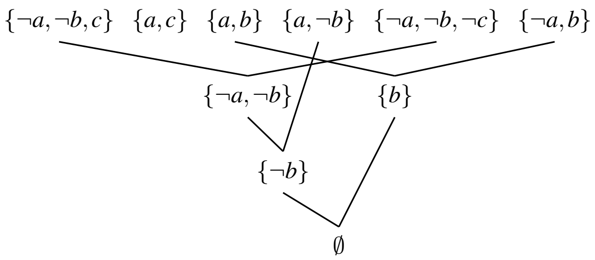
$$(b \vee a \vee d) \wedge (a \vee \neg d) \wedge (\neg b \vee c) \wedge (\neg c \vee b) \wedge (b \vee \neg a \vee c) \\ \wedge (\neg b \vee a) \wedge (\neg a \vee \neg c).$$

Der Resolutionsbeweis:



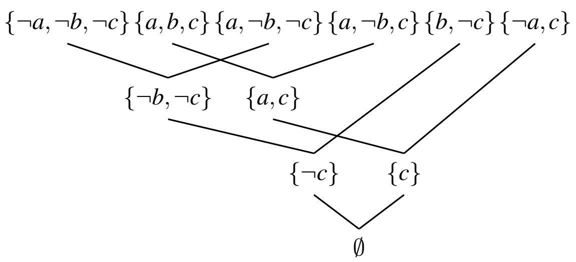
Lösung zu 6.8

Der Beweis im Resolutionskalkül lautet:



Lösung zu 6.9

Die Formel ist eine Tautologie genau dann, wenn ihre Negation eine Kontradikation ist. Nun gilt für den ersten Formelteil $(a \wedge b) \to \neg c \equiv \neg(a \wedge b) \vee \neg c \equiv \neg a \vee \neg b \vee \neg c$. Der Beweis im Resolutionskalkül lautet dann:



7-1

Kapitel 7
Hilbertkalkül der Aussagenlogik

Axiome + Modus ponens = gutes Beweissystem

7-2

Lernziele dieses Kapitels

1. Begriff der Ableitung in Hilbertkalkülen verstehen und anwenden können
2. Das Deduktionstheorem und seinen Beweis verstehen

Inhalte dieses Kapitels

Worum es heute geht

Mathematiker versuchen Tag ein, Tag aus herauszufinden, ob bestimmte Formeln Tautologien sind. Immer, wenn ihnen das gelingt (und es noch niemand anderem gelungen ist), dann sind sie ganz aufgeregt und schreiben die Formel ganz schnell auf ein Papier, gefolgt von einer Begründung, weshalb die Formel eine Tautologie ist. Um herauszustreichen, dass ihnen die Tautologie besonders wichtig und tiefschürfend erscheint, nennen sie die Formel einen »Satz«; die Begründung, weshalb die Formel eine Tautologie ist, nennen sie einen »Beweis«. Ihren Satz schicken sie dann an andere Mathematiker. Wenn diese den Satz genauso aufregend finden, kann der Satz sogar den Namen seines Entdeckers bekommen, was diesen dann wirklich ganz doll freut.

Die Bezeichnung »Satz« ist übrigens ausgesprochen irreführend, dies ist in typischer Fall, wo Mathematiker ein unschuldiges deutsches Wort genommen haben und es nun für ihre eigenen, je nach Standpunkt üblen oder hehren, Ziele gebrauchen. Ähnlich ergangen ist es dem »Ring«, unter dem Mathematikerinnen weder eine runde Scheibe mit einem Loch in der Mitte verstehen, die man sich typischerweise an Finger steckt, noch einen etwas zu lang und pathetisch geratenen Opernzyklus.

Warum freuen sich Mathematiker denn so, wenn sie einen Satz bewiesen haben? So spannend ist der Umstand, dass $a \vee (b \vee \neg b)$ eine Tautologie ist, nun auch wieder nicht. Das Schöne an Sätzen ist, dass man sie in Beweisen von neuen Sätzen benutzen kann. Deshalb finden Sie in Beweisen oft Formulierungen wie »… und nun folgt nach dem Satz von Bolzano-Weierstraß, dass… «, so dass über die Jahre, Jahrzehnte, Jahrhunderte und Jahrtausende immer komplexere Sätze bewiesen werden können. Der Satz des Pythagoras mag vor zweitausend Jahren noch sehr aufregend gewesen sein, heute lernt man das in der Schule. In tausend Jahren werden sich wahrscheinlich Lehrplanverantwortlichen für die Vorschule darüber streiten, ob das PCP-Theorem nicht lieber doch erst in der ersten Schulklasse unterrichtet werden sollte.

Wenn also Mathematiker normalerweise Tautologien beweisen, indem sie aus bereits bekannte Tautologien neue Tautologien folgern, was liegt näher, als ein formales Beweissystem aufzubauen, das genauso funktioniert? Der *Hilbertkalkül der Aussagenlogik* leistet genau dieses: Ausgangspunkt sind einige wenige so genannte *Axiome*, welche ganz einfache

Tautologien sind. Es gibt eine Regel, den *Modus ponens*, nach der man neue Tautologien folgern darf: Wenn φ eine Tautologie ist und $\varphi \to \psi$ auch, so auch ψ. Mehr ist nicht nötig, um *alle aussagenlogische Tautologien* zu beweisen.

7.1 Hilbertkalkül

7.1.1 Ziel: Ein Beweissystem

Der Hilbertkalkül 7-4

Problemstellung

Wir wollen beweisen, dass eine Formel eine Tautologie ist, wobei die Formel nur die Junktoren $\to$ und $\neg$ enthält.

Das Beweissystem »Hilbertkalkül«

In diesem System sind *Beweise* gerade *Folgen von Tautologien*. Die *letzte Formel* muss gerade die Behauptung sein. Jede Formel im Beweis muss durch eine der folgenden Regeln gebildet werden:

1. Die Formel ist eines der *Axiome* des Systems.
2. Die Formel ist durch Anwendung des *Modus ponens* aus zwei Formeln weiter vorne entstanden.

7.1.2 Axiome

Was sind Axiome? 7-5

▶ Definition: Axiom, Axiomensystem

1. Ein *Axiom* ist eine Tautologie von einer bestimmten Form.
2. Ein *Axiomensystem* ist eine Menge von Axiomen.

Axiomensystem nach Mendelson

Folgende Formeln sind Axiome, wobei φ_1, φ_2 und φ_3 beliebige Formeln sind:

I $\varphi_1 \to (\varphi_2 \to \varphi_1)$
II $\big(\varphi_1 \to (\varphi_2 \to \varphi_3)\big) \to \big((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\big)$
III $(\neg\varphi_2 \to \neg\varphi_1) \to \big((\neg\varphi_2 \to \varphi_1) \to \varphi_2\big)$

7.1.3 Modus ponens

Was ist der Modus ponens? 7-6

▶ Definition

Die *Regel Modus ponens* (*modus*: lateinisch »Schlussfigur«, *ponere* lateinisch »stellen, setzen«) erlaubt es, aus zwei Zeilen, die φ und $\varphi \to \psi$ lauten, die neue Zeile ψ zu bilden.

7.1.4 Beispiele

7-7 **Ein Beweis im Beweissystem »Hilbertkalkül«.**

Behauptung
Die Formel $a \to a$ ist eine Tautologie.

Beweis.

1. $a \to ((a \to a) \to a)$
   (Axiom I für $\varphi_1 = a$ und $\varphi_2 = (a \to a)$)
2. $\big(a \to ((a \to a) \to a)\big) \to \big((a \to (a \to a)) \to (a \to a)\big)$
   (Axiom II für $\varphi_1 = a$, $\varphi_2 = (a \to a)$ und $\varphi_3 = a$)
3. $(a \to (a \to a)) \to (a \to a)$
   (Modus ponens auf 1. und 2.)
4. $(a \to (a \to a))$
   (Axiom I für $\varphi_1 = a$ und $\varphi_2 = a$)
5. $(a \to a)$
   (Modus ponens auf 4. und 3.)

7-8 **Stimmt der Beweis wirklich?**
Der Beweis von eben *scheint richtig*. Jedoch ist es ja zumindest *vorstellbar,* dass durch einen Tippfehler etwas doch nicht stimmt. Schöner wäre es, wenn der Beweis durch einen Computer überprüft würde. Genau dies kann man auch machen lassen, siehe dazu die Webseite des MetaMath-Projektes, dort Theorem id1 (http://us.metamath.org/).

7-9 ✎ **Zur Übung**
Geben Sie einen Beweis im Hilbertkalkül dafür an, dass folgende Formel eine Tautologie ist:

$$(a \to \neg a) \to (a \to a)$$

Die Axiome lauteten:

- I $\varphi_1 \to (\varphi_2 \to \varphi_1)$
- II $\big(\varphi_1 \to (\varphi_2 \to \varphi_3)\big) \to \big((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\big)$
- III $(\neg\varphi_2 \to \neg\varphi_1) \to \big((\neg\varphi_2 \to \varphi_1) \to \varphi_2\big)$

7-10 **Werbeseite für den Hilbertkalkül.**
Der Hilbertkalkül ist flexibel, da das Axiomensystem variiert werden kann. Hat man einmal eine Tautologie wie $(a \to a)$ bewiesen, so kann man sie jederzeit »wieder hervorholen«. Man kann sich so eine *Bibliothek nützlicher Tautologien* aufbauen. Bereits bewiesene Tautologien muss man dann nicht jedesmal neu beweisen, sondern schreibt »$(a \to a)$ (wie auf Seite 1234 gezeigt)«.
Das »Anhäufen von Tautologien« entspricht genau dem Vorgehen von Mathematikern: *Sätze* sind eigentlich nur komplizierte Tautologien. Mathematiker bauen seit Jahrhunderten eine *große Bibliothek nützlicher Tautologien auf*. In Beweisen schreibt man beispielsweise »nach dem Satz von Bolzano-Weierstraß gilt nun…«.

✎ **Zur Diskussion**
Was spricht gegen den Hilbertkalkül?

7.2 Ableitungen

7.2.1 Beweise mit Voraussetzungen

Neues Ziel: Beweise mit Voraussetzungen. 7-11

Eben wurde behauptet, Beweise bestünden aus langen Folgen von Tautologien. In echten Beweise werden aber oft Annahmen gemacht, die gar nicht allgemeingültig sind.

Beispiele

- *»Es gelte $\beta \models \varphi$. Dann gilt $\hat{\beta}(\varphi) = 1$. Also …«*
  (Es ist gerade nicht jedes β ein Modell von φ.)
- *»For the sake of contradiction, assume that a 4-vertex tournament T with diameter 2 exists. Clearly, …«*
  (Ein solches Tournament T existiert gerade nicht.)

7.2.2 Der Ableitungsbegriff

Hilbert-Beweise mit Voraussetzungen. 7-12

Wir *erweitern* den Hilbertkalkül, indem wir erlauben, dass im Beweis auch *klar benannte Voraussetzungen* benutzt werden.

▶ **Definition**

Sei Φ eine Menge von Formeln (nicht notwendig Tautologien). Diese nennen wir *Voraussetzungen*. Ein *Hilbertbeweis* einer Formel ψ *unter diesen Voraussetzungen* ist eine Folge von Formeln, so dass jede durch eine der folgenden Regeln gebildet wurde:

1. Die Formel ist eines der *Axiome* des Systems.
2. Die Formel ist eine der *Voraussetzungen*, also ein Element von Φ.
3. Die Formel ist durch Anwendung des *Modus ponens* auf zwei Formeln weiter vorne entstanden.

Die letzte Formel in der Reihe muss wieder gerade ψ sein. Wir sagen dann, *ψ lässt sich aus Φ ableiten*.

Beispiel und Aufgabe 7-13

Beispielbeweis
Aus $\{\neg a \to \neg b, \neg a \to b\}$ lässt sich a ableiten:

1. $(\neg a \to \neg b) \to \big((\neg a \to b) \to a\big)$
   (Axiom III für $\varphi_2 = a$ und $\varphi_1 = b$)
2. $(\neg a \to \neg b)$
   (Voraussetzung)
3. $(\neg a \to b) \to a$
   (Modus ponens auf 1. und 2.)
4. $(\neg a \to b)$
   (Voraussetzung)
5. a
   (Modus ponens auf 3. und 4.)

✎ **Zur Übung**

Wie lässt sich aus $\{a, b\}$ die Formel $b \to a$ ableiten?

Schreibweisen. 7-14

Notation

Lässt sich ψ aus Φ ableiten, so schreiben wir

$$\Phi \vdash \psi.$$

Statt $\emptyset \vdash \psi$ schreiben wir

$$\vdash \psi.$$

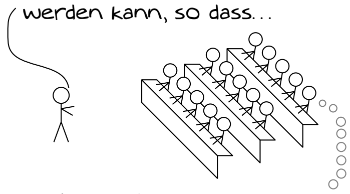
Bemerkungen:

- $\vdash \psi$ bedeutet, dass sich ψ ohne Voraussetzungen zeigen lässt. In einem solchen Beweis gibt es also nur Tautologien.
- Das Wort »ableiten« benutzt man auch bei Grammatiken, wo es aber etwas anderes bedeutet.

7.2.3 Das Deduktionstheorem

Wie man Voraussetzungen los wird.

7-16 Nach dem Deduktionstheorem existiert also ein Beweis der Kontraposition, wenn auf eine Formel der Prämissenmenge der Modus ponens angewendet werden kann, so dass…



In dem Werbeflyer stand, dieses Studium würde mich optimal auf meine Arbeit als Software-Entwicklerin vorbereiten…

▶ Satz: Deduktionstheorem
Es sei Φ eine Menge von Formeln und φ sei eine Formel. Es gelte $\Phi \cup \{\varphi\} \vdash \psi$. Dann gilt auch $\Phi \vdash \varphi \to \psi$.

- Das Deduktionstheorem ist eine Aussage *über formale Beweise*.
- »$\Phi \cup \{\varphi\} \vdash \psi$« bedeutet, dass man ψ formal beweisen kann, wenn alle Formeln in Φ und auch φ als Voraussetzungen in dem formalen Beweis benutzen darf.
- »$\Phi \vdash \varphi \to \psi$« bedeutet, dass man $\varphi \to \psi$ formal beweisen kann, *ohne* die Voraussetzung φ zur Verfügung zu haben.

Beispiel
Es galt $\{\neg a \to \neg b, \neg a \to b\} \vdash a$. Also gilt auch $\{\neg a \to \neg b\} \vdash (\neg a \to b) \to a$.

7-17 ### Beweis des Deduktionstheorems.

Kommentare zum Beweis

Beweis. Wir führen einen *konstruktiven Beweis*. Es gelte $\Phi \cup \{\varphi\} \vdash \psi$ und es sei ψ_1, ψ_2, …, ψ_n ein formaler Beweis für ψ. Wir konstruieren einen formalen Beweis für $\varphi \to \psi$.[1]
In dem formalen Beweis zeigen wir nacheinander $\varphi \to \psi_1$, dann etwas später $\varphi \to \psi_2$, dann $\varphi \to \psi_3$ und so weiter, bis wir schließlich $\varphi \to \psi_n$ gezeigt haben (was ja gerade gleich $\varphi \to \psi$ ist).

Alter formaler Beweis
Voraussetzungen: $\Phi \cup \{\varphi\}$

1. ψ_1
2. ψ_2
3. …
4. ψ_n

Neuer formaler Beweis
Voraussetzungen: Φ

1. …
2. $\varphi \to \psi_1$
3. …
4. $\varphi \to \psi_2$
5. …
6. $\varphi \to \psi_n$

Jede Zeile ψ_i im alten Beweis wird wie folgt ersetzt:

- Ist ψ_i eines der Axiome oder $\psi_i \in \Phi \setminus \{\varphi\}$, so ersetze es durch:
  1. ψ_i (Axiom oder Voraussetzung)
  2. $\psi_i \to (\varphi \to \psi_i)$ (Axiom I)
  3. $\varphi \to \psi_i$ (mp)
- Ist $\psi_i = \varphi$, so ersetze die Zeile durch:
  1. $\varphi \to ((\varphi \to \varphi) \to \varphi)$ (Axiom I)
  2. $\big(\varphi \to ((\varphi \to \varphi) \to \varphi)\big) \to \big((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)\big)$ (Axiom II)
  3. $(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$ (mp)
  4. $(\varphi \to (\varphi \to \varphi))$ (Axiom I)
  5. $(\varphi \to \varphi)$ (mp)
- Ist ψ_i durch Modus ponens aus den Zeilen ψ_k und $\psi_k \to \psi_i$ hervorgegangen, so ersetzen wir die Zeile durch:
  1. $(\varphi \to (\psi_k \to \psi_i)) \to ((\varphi \to \psi_k) \to (\varphi \to \psi_i))$ (Axiom II)
  2. $(\varphi \to \psi_k) \to (\varphi \to \psi_i)$ (mp)
  3. $\varphi \to \psi_i$ (mp)

  Beachte: Die Zeilen $\varphi \to (\psi_k \to \psi_i)$ und $\varphi \to \psi_k$ gibt es schon.

Nach der *Konstruktion* muss man nun noch zeigen, dass das konstruierte Objekt die behaupteten Eigenschaften hat.[2] Das konstruierte Objekt ist aber offenbar[3] ein formaler Beweis von $\varphi \to \psi$, in dem die Formel φ nicht als Voraussetzung benutzt wird. □

[1] Jetzt kommt die Konstuktion.

[2] Gut, dass das nicht wie üblich vergessen wird.

[3] Schlecht, dass hier nur »offenbar« steht. Es wäre hier ein Induktionsbeweis angebracht gewesen.

Zusammenfassung dieses Kapitels

▶ Hilberkalkül 7-18

Beweise im vollständigen und korrekten Beweissystem »Hilbertkalkül« sind so aufgebaut:

- Jede Zeile ist ein *Axiom*, eine *Anwendung des Modus ponens* oder eine *Voraussetzung*.
- Die letzte Zeile ist die zu beweisende Formel.

Man schreibt $\Phi \vdash \psi$, falls es einen Hilbert-Beweis für ψ unter den Voraussetzungen Φ gibt.

▶ Deduktionstheorem

Falls $\Phi \cup \{\varphi\} \vdash \psi$, so auch $\Phi \vdash \varphi \to \psi$.

▶ »Hauptsatz« der Aussagenlogik

$\Phi \models \psi$ gilt genau dann, wenn $\Phi \vdash \psi$.

Zum Weiterlesen

[1] Elliot Mendelson, *Introduction to Mathematical Logic,* Chapman & Hall, 1997

Das Axiomsystem für die Aussagenlogik, das in dieser Vorlesung verwendet wird, stammt hieraus.

[2] MetaMath Website, *Theorem id1,* http://us.metamath.org/mpegif/id1.html, Zugriff Dezember 2011

Hier findet man einen maschinell überprüften Beweis der Tautologie $\varphi \to \varphi$. Der Besuch der Webseite ist aber auch sonst sehr interessant.

Übungen zu diesem Kapitel

Übung 7.1 Einen Hilbertbeweis führen, mittel

In dieser Aufgabe betrachten wir einen Hilbertkalkül, der zusätzlich zu den Mendelson-Axiomen noch die folgenden enthält (φ, φ_1 und φ_2 sind beliebige Formeln):

IV $\varphi_1 \wedge \varphi_2 \to \varphi_2$,
V $\neg\neg\varphi \to \varphi$.

Als Schlussregel ist weiterhin nur *Modus Ponens* erlaubt.

1. Zeigen Sie, dass die neuen Axiome Tautologien sind.
2. Zeigen Sie in diesem erweiterten Kalkül, dass die Formel $\neg\neg(b \wedge c) \to c$ eine Tautologie ist.

Tipp: Verwenden Sie Axiom II mit $\varphi_1 = \neg\neg(b \wedge c)$, $\varphi_2 = b \wedge c$ und $\varphi_3 = c$.

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

Prüfungsfrage 7.2

12 min

→ Lösung

Einen Hilbertbeweis nachvollziehen

Das Mendelson'sche Axiomensystem hat folgende drei Axiome:

I $\varphi \to (\psi \to \varphi)$
II $\big(\varphi \to (\psi \to \rho)\big) \to \big((\varphi \to \psi) \to (\varphi \to \rho)\big)$
III $(\neg\varphi \to \neg\psi) \to \big((\neg\varphi \to \psi) \to \varphi\big)$

Im Folgenden ist ein Hilbert-Kalkül-Beweis für

$$\{\neg a \to \neg b, b \to a\} \vdash (\neg a \to b) \to a$$

angegeben. Geben Sie für jede Zeile des Beweises an, ob es sich bei der Zeile um eine Voraussetzung handelt, um eines der Axiome (und wenn ja, welches) oder um eine Anwendung des Modus ponens (und wenn ja, auf welche Zeilen er angewandt wurde).

1. $(\neg a \to \neg b) \to ((b \to a) \to (\neg a \to \neg b))$
2. $\neg a \to \neg b$
3. $(\neg a \to \neg b) \to ((\neg a \to b) \to a)$
4. $(b \to a) \to (\neg a \to \neg b)$
5. $b \to a$
6. $\neg a \to \neg b$
7. $(\neg a \to b) \to a$

Geben Sie nun einen Beweis für $\{\neg a \to \neg b, b \to a\} \vdash (\neg a \to b) \to a$ an, der mit nur drei Zeilen auskommt.

Prüfungsfrage 7.3

10 min

Einen Hilbertbeweis nachvollziehen

Der folgende Beweis im Hilbertkalkül mit Mendelsons Axiomensystem zeigt, dass $\{b \vee c \to \neg\neg(b \vee c), b \to b \vee c\} \vdash b \to \neg\neg(b \vee c)$ gilt. Zeigen Sie die Korrektheit des Beweises, indem Sie für jede Zeile angeben, warum sie an dieser Stelle erlaubt ist.

1. $b \vee c \to \neg\neg(b \vee c)$
2. $(b \vee c \to \neg\neg(b \vee c)) \to (b \to ((b \vee c) \to \neg\neg(b \vee c)))$
3. $b \to ((b \vee c) \to \neg\neg(b \vee c))$
4. $(b \to ((b \vee c) \to \neg\neg(b \vee c))) \to ((b \to (b \vee c)) \to (b \to \neg\neg(b \vee c)))$
5. $(b \to b \vee c) \to (b \to \neg\neg(b \vee c))$
6. $b \to b \vee c$
7. $b \to \neg\neg(b \vee c)$

Prüfungsfrage 7.4

14 min

→ Lösung

Beweis im Hilbert-Kalkül vervollständigen

Wir betrachten folgenden unvollständigen Beweis für

$$\{\neg\neg b \to \neg\neg(c \wedge d), \neg(c \wedge d)\} \vdash \neg b$$

im Hilbert-Kalkül:

1.	$\neg\neg b \to \neg\neg(c \wedge d)$	Voraussetzung
2.	?	?
3.	$(\neg\neg b \to \neg(c \wedge d)) \to \neg b$	modus pones auf 1,2
4.	$\neg(c \wedge d) \to (\neg\neg b \to \neg(c \wedge d))$	Axiom I
5.	?	?
6.	$\neg\neg b \to \neg(c \wedge d)$	modus pones auf 4,5
7.	?	?

Vervollständigen Sie die Zeilen 2, 5 und 7 dieses Beweises und geben Sie für diese Zeilen an, welches Axiom, welche Voraussetzung oder Regel Sie dabei benutzt haben.

Lösung zu 7.2

1. $(\neg a \to \neg b) \to ((b \to a) \to (\neg a \to \neg b))$
   Axiom I
2. $\neg a \to \neg b$
   Voraussetzung
3. $(\neg a \to \neg b) \to ((\neg a \to b) \to a)$
   Axiom III
4. $(b \to a) \to (\neg a \to \neg b)$
   Modus ponens auf 1. und 3.
5. $b \to a$
   Voraussetzung
6. $\neg a \to \neg b$
   Modus ponens auf vorherigen beiden Zeilen
7. $(\neg a \to b) \to a$
   Modus ponens auf 3. und vorherige Zeile

Ein kurzer Beweis lautet:

1. $(\neg a \to \neg b) \to ((\neg a \to b) \to a)$
2. $(\neg a \to \neg b)$
3. $(\neg a \to b) \to a$

Lösung zu 7.4

Der vollständigen Beweis für

$$\{\neg\neg b \to \neg\neg(c \wedge d), \neg(c \wedge d)\} \vdash \neg b$$

im Hilbert-Kalkül lautet:

1. $\neg\neg b \to \neg\neg(c \wedge d)$
   Voraussetzung
2. $(\neg\neg b \to \neg\neg(c \wedge d)) \to ((\neg\neg b \to \neg(c \wedge d)) \to \neg b)$
   Axiom III
3. $(\neg\neg b \to \neg(c \wedge d)) \to \neg b$
   Modus pones auf 1,2
4. $\neg(c \wedge d) \to (\neg\neg b \to \neg(c \wedge d))$
   Axiom I
5. $\neg(c \wedge d)$
   Voraussetzung
6. $\neg\neg b \to \neg(c \wedge d)$
   modus pones auf 4,5
7. $\neg b$
   Modus ponens auf 3,6

8-1

Kapitel 8
Der Hilbertkalkül der Aussagenlogik ist vollständig
Eine mathematische Cocktailparty

8-2

Lernziele dieses Kapitels

1. Die wesentlichen Schritte des Beweises des Vollständigkeitssatzes des Hilbertkalküls beschreiben können
2. Einen nichtkonstruktiven Existenzbeweis kennen
3. Die Vollständigkeit von Axiomsystemen einschätzen können

Inhalte dieses Kapitels

Worum es heute geht

Wir haben in den letzten drei Kapiteln drei Beweissysteme kennengelernt: die *Wahrheitstafeln*, die *Resolution* und den *Hilbertkalkül*. Alle drei dienen dazu, *Beweise* so aufzuschreiben, dass es »wirklich einfach« ist zu überprüfen, ob der Beweis stimmt oder nicht. Man kann sicherlich mit einigem Recht behaupten, dass alle drei Systeme diesem Anspruch gerecht werden.

Wie leicht es hingegen ist, Beweise zu *finden,* steht auf einem ganz anderen Blatt. Für die Wahrheitstafeln ist das Finden natürlich schon fast lächerlich einfach: Einfach alle möglichen Belegungen für die Variablen untereinanderschreiben und rechts immer eine 1. Einfacher geht es nicht. Bei der Resolution ist die Sache schon etwas schwieriger, es gibt verschiedene Möglichkeiten und Reihenfolgen, in denen man eine Resolution durchführen kann. Jedoch gilt auch hier: Man kann eigentlich nichts falsch machen, denn früher oder später stößt man automatisch auf den Beweis.

Für den Hilbertkalkül ist das Finden von Beweisen leider ausgesprochen schwierig. Wenn man einfach mal »drauflosbeweist«, dann wird man in der Regel alles mögliche zeigen, aber nicht die Behauptung. Mit einer gehörigen Portion Geschick kann man ein Programm schreiben, dass systematisch alle möglichen Beweise durchgeht und früher oder später einen Beweis findet – wenn er denn existiert, womit wir beim Thema dieses Kapitels wären.

War es für das Beweissystem »Wahrheitstafel« noch unmittelbar klar, dass immer ein Beweis für jede Tautologie existiert, war es für die Resolution schon deutlich aufwändiger, dies zu zeigen. Das Argument für die Resolution ging, grob gesprochen wie folgt: Der gesuchte formale Beweis für eine gegebene Tautologie ergibt sich einfach durch die konsequente Anwendung der Resolutionsregel »bis es nicht mehr geht«. Die Schwierigkeit war dann zu zeigen, dass dies tatsächlich einen formalen Beweis darstellt. Nochmal langsam und zum Mitschreiben: Bei der Resolution ist die *Konstruktion* eines formalen Beweises einfach, es ist schwierig zu zeigen, *dass dies ein formaler Beweis ist.*

Beim Hilbertkalkül ist es nun leider völlig unklar, wie man zeigen soll, dass es zu jeder Tautologie einen Beweis gibt. Beispielsweise war das Axiomsystem von Gottlob Frege, der als erster überhaupt ein Axiomsystem für die Aussagenlogik vorgeschlagen hat, bereits vollständig – er schaffte es aber nicht, dies zu zeigen.

Für die Aussagenlogik gibt es zwei Arten, wie man zeigen kann, dass es doch für jede Tautologie einen formalen Beweis gibt:

1. Man gibt ein algorithmisches Verfahren an, wie man den Beweis findet. Dann muss man argumentieren, dass dieses Verfahren immer funktioniert.
2. Man führt einen Widerspruchsbeweis, indem man annimmt, es gäbe keinen Beweis und dies zu einem Widerspruch führt.

Beide Methoden führen zum Erfolg, wir werden aber nur die zweite betrachten. Dies hat zwei Gründe: Zum einen funktioniert die erste Methode wirklich *nur* für die Aussagenlogik, wohingegen die zweite auch bei der Prädikatenlogik funktioniert, die wir in den folgenden Kapiteln kennen lernen werden. Zum anderen ist die zweite einfacher und nutzt ein neues Beweisrezept: Es handelt sich um einen *nichtkonstruktiven* Beweis.

8.1 Einleitung: Beweise finden

8-4 Die drei Beweissysteme, die wir kennen gelernt haben.

Beweissystem Wahrheitstafel
Beweise sind *Tabellen, in denen rechts immer eine 1 steht.*

Beweissystem Resolution
Beweise sind *Folgen von Formeln in KNF; jede geht durch Resolution aus vorherigen hervor.*

Beweissystem Hilbertkalkül
Beweise sind *Folgen von Tautologie; jede ist ein Axiom oder geht durch Modus ponens aus vorherigen hervor.*

✎ **Zur Diskussion**

1. Wie schwierig ist es jeweils *Beweise zu überprüfen?*
2. Wie schwierig ist es jeweils *Beweise zu finden?*

8-5 Wiederholung: Der Kalkül, um den es geht.

▶ **Definition**
Sei Φ eine Menge von Formeln und ψ eine Formel. Wir schreiben $\Phi \vdash \psi$ und sagen ψ *lässt ich aus* Φ *ableiten,* wenn es eine Folge von Formeln gibt, die mit ψ endet und für jede gilt mindestens einer der folgenden Punkte:

1. Die Formel ist eines der folgenden *Axiome* des Systems:
   I $\varphi_1 \to (\varphi_2 \to \varphi_1)$
   II $\big(\varphi_1 \to (\varphi_2 \to \varphi_3)\big) \to \big((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\big)$
   III $(\neg\varphi_2 \to \neg\varphi_1) \to \big((\neg\varphi_2 \to \varphi_1) \to \varphi_2\big)$

   Hierbei sind φ_1, φ_2 und φ_3 beliebige Formeln.
2. Die Formel ist eine der *Voraussetzungen* (ein Element von Φ).
3. Die Formel ist durch Anwendung des *Modus ponens* auf zwei Formeln weiter vorne entstanden.

8.2 Korrektheit

Korrektheit des Hilbert-Kalküls. 8-6

▶ Satz

Der Hilbertkalkül mit den Axiomen von Mendelson ist korrekt.

Beweis. Es genügt zu zeigen, dass ein Hilbertbeweis (ohne Voraussetzungen) nur aus Tautologien besteht. Dies zeigt man durch Induktion über die Länge des Beweises.
Den Induktionsanfang macht die Länge 0. Für einen leeren Beweis ist nichts zu zeigen. Sei nun ein Beweis der Länge n gegeben, der nur aus Tautologien besteht, der nun um eine $(n+1)$-te Formel ψ ergänzt wird. Ist diese eines der Axiome, so ist sie eine Tautologie (wie man durch eine Wahrheitstafel leicht sieht). Ist sie durch den Modus ponens zweier vorhergehenden Zeilen φ und $\varphi \to \psi$ entstanden, so waren diese nach Voraussetzung Tautologien. Dann ist aber auch ψ eine. □

Es gilt noch etwas mehr. 8-7

Der Satz über die Korrektheit des Hilbertkalküls sagt nur etwas über Ableitungen *ohne Voraussetzungen* aus. Tatsächlich gilt aber folgender stärker Satz:

▶ Satz

Sei Φ eine Menge von Formeln und ψ eine Formel.

$$\textit{Falls } \Phi \vdash \psi, \textit{ so gilt } \Phi \models \psi.$$

✎ Zur Diskussion

Wieso ist dieser Satz »stärker« als der Korrektheitssatz?

Beweis. Nach Voraussetzung gibt es eine Ableitung $\varphi_1, \varphi_2, \dots, \varphi_n$ von ψ aus Φ.[1] Sei β ein Modell von Φ.[2] Wir zeigen durch Induktion über n, dass β ein Modell von allen φ_i ist und damit auch von $\varphi_n = \psi$.
Für $n = 0$ ist nichts zu zeigen. Ist nun β ein Modell aller φ_i mit $i < n$, so auch von φ_n:

- Ist φ_n ein Axiom, so ist es eine Tautologie und damit sind alle Welten Modelle, insbesondere auch β.
- Ist $\varphi_n \in \Phi$, so haben wir angenommen, dass β ein Modell ist.
- Ist φ_n durch Modus ponens entstanden, so war nach Induktionsvoraussetzung β Modell sowohl von φ_i und von $\varphi_i \to \varphi_n$ für ein geeignetes i. Dann muss β auch ein Modell von φ_n sein.

□

Kommentare zum Beweis

[1] Es galt ja $\Phi \vdash \psi$, was genau das aussagt.

[2] Rezept All-Aussagen beweisen: $\Phi \models \psi$ bedeutet: Jedes Modell von Φ ist ein Modell von ψ.

8.3 Vollständigkeitssatz

Die Schwierigkeiten beim Beweis des Vollständigkeitssatzes für den Hilbertkalkül der Aussagenlogik. 8-8

Anders als bei Wahrheitstafeln und Resolution ist es *sehr schwierig,* Hilbert-Beweise zu *finden*. Speziell für die Aussagenlogik *gibt es zwar einen Algorithmus,* der Beweise »berechnet«, jedoch ist er *kompliziert* und auch *nur* bei der Aussagenlogik anwendbar. Wir werden deshalb *anders, indirekter* vorgehen und eine Methodik benutzen, die auch später bei der Prädikatenlogik funktioniert.

8.3.1 Der Satz

8-9 Das Axiomensystem ist vollständig.

▶ Satz
Der Hilbertkalkül mit den Axiomen von Mendelson ist vollständig.

(Genauer gilt die Vollständigkeit nur, wenn man sich auf Formeln beschränkt, in denen lediglich die Junktoren $\neg$, $\to$ und Variablen vorkommen. Das ließe sich aber durch ein paar weitere Axiome leicht beheben.)
Genau wie eben ist dieser Satz nur ein *Spezialfall* von einem anderen Satz:

▶ Satz
Sei Φ eine Menge von Formeln und ψ eine Formel.

$$\textit{Falls } \Phi \models \psi, \textit{ so gilt } \Phi \vdash \psi.$$

8-10 Von der Mathematik zur Cocktail-Party.
Auf Ihrer nächsten Party wollen Sie neuen Cocktail herstellen: Den Psi-Cocktail! Den gab es letztens auf einer total coolen Party bei einer Freundin. Sie haben vorsichtshalber schon alle Zutaten gekauft, die Ihre genutzt Freundin hatte. Sie hat Ihnen dazu eine Liste gegeben, die wir mal Φ nennen wollen. Leider wissen Sie nicht, wie sie aus den Zutaten in Φ den Psi-Cocktail herstellen können. Sie brauchen ein Rezept! Allerdings darf es nicht zu kompliziert sein, da Sie kein sonderlich erfahrener Cocktail-Mixer sind. Jeder Schritt auf dem Rezept muss schön einfach sein.

8-11 Wie wir mathematische Begriffe in Cocktails übersetzen.

Mathematik	*»Übersetzung«*
Φ	Die Menge der »Zutaten«
ψ	Der zu mixende Cocktail
Ableitung	Cocktail-Rezept, das Sie ausführen können
$\Phi \vdash \psi$	Es gibt ein »Anfänger-Cocktail-Rezept«, um einen Psi-Cocktail aus den Zutaten in Φ herzustellen
$\Phi \models \psi$	Irgendwer (Ihre Freundin) hat es irgendwie geschafft, einen Psi-Cocktail aus den Zutaten in Φ herzustellen; aber vielleicht mit Geräten, die Sie nicht haben

8.3.2 Der Beweisplan

8-12 Was wir machen müssen und was wir nicht machen werden.
Die zu beweisende Aussage ist von folgender Form:

> Wenn ... gilt, so gilt $\Phi \vdash \psi$.

Das kann man auch anders schreiben:

> Wenn ... gilt, so *gibt es* eine Ableitung, die Φ als Voraussetzungen nutzt und mit ψ endet.

Es wäre nun *sehr natürlich,* das Beweisrezept »Konstruktiver Beweis« anzuwenden: Wir sollen ja zeigen, dass es eine bestimmte Art Ableitung *gibt*. Das *werden wir aber nicht tun.* Vielmehr werden wir einen Widerspruchsbeweis führen und annehmen, es *gäbe keine Ableitung,* was später zu einem Widerspruch führt.

8-13 Was das für Ihre Cocktailparty bedeutet.
Die zu beweisende Aussage ist von folgender Form:

> Wenn Ihre Freundin aus den Zutaten in Φ einen Psi-Cocktail gemixt bekommt, dann gibt es ein Anfängerrezept, um aus den Zutaten in Φ einen Psi-Cocktail zu mixen.

Es wäre nun *sehr natürlich,* anzugeben, wie das Cocktail-Rezept lautet. Das *werden wir aber nicht tun.* Vielmehr werden wir einen Widerspruchsbeweis führen und annehmen, es *gäbe kein Anfängerrezept, das Sie ausführen können,* was später zu einem Widerspruch führt.

Beweisrezept: *Widerspruchsbeweis* 8-14

Ziel
Eine Behauptung beweisen, indem man zeigt, dass die Annahme des Gegenteils zu einem Widerspruch führt.

Rezept

1. Leite den Beweis mit »Wir führen einen Widerspruchsbeweis.« oder »Zum Zwecke des Widerspruchs nehmen wir an, dass B nicht gilt.«
2. Führe nun einen Beweis, in dem die Annahme »nicht B« beliebig benutzt werden darf.
3. Versuche, die ursprüngliche Behauptung »B« herzuleiten oder eine offensichtlich falsche Behauptung wie $1 = 2$.
4. Beende den Beweis, wenn dies gelungen ist, mit »Widerspruch.« oder mit »Dies ist aber ein Widerspruch zur Annahme, dass nicht B gilt, deshalb muss B doch gelten«.

Beweisrezept: *Nichtkonstruktive Beweise mittels Widerspruch* 8-15

Ziel
Es soll gezeigt werden, dass es ein Ding mit bestimmten Eigenschaften gibt.

Rezept

1. Beginne mit »Wir führen einen nichtkonstruktiven Beweis. Nehmen wir dazu an, dass es kein ... gäbe, das Eigenschaften ... hat.«
2. Man zeigt nun, dies zu einem Widerspruch führt. Ende diesen Teil mit »Dies ist ein Widerspruch.«
3. Ende den Beweis mit »Die Annahme, dass es kein ... gäbe, hat zu einem Widerspruch geführt. Folglich gibt es ein ....«

Man beachte: Aus dem Beweis *wird in aller Regel nicht klar, wie man ein Ding finden könnte, das die behaupteten Eigenschaften hat,* weshalb man *konstruktive* Beweise bevorzugt.

Beweisrezept: *Beweise strukturieren* 8-16

Ziel
Der Leser soll immer genau wissen, was bereits gezeigt wurde und was noch zu zeigen ist.

Rezept
Beweise werden schnell »unübersichtlich«. Abhilfe:

- Benutzen Sie Wendungen wie »Damit wurde gezeigt, dass ...« oder »Es bleibt zu zeigen, dass ...« oder »Im Folgenden zeigen wir zunächst ..., ... zeigen wir hingegen später.«
- Geben Sie am Anfang eines langen Beweises eine Übersicht und teilen Sie den Beweis in Abschnitte wie »Die Konstruktion« oder »Die Rückrichtung der Korrektheit der zweiten Unterkonstruktion«.
- Formulieren Sie Zwischenbehauptung als Lemmata, die Sie zuerst beweisen.

Grundideen des Beweises 8-17
Es gibt zwei Annahmen:

A $\Phi \models \psi$. Das war eine Voraussetzung im Satz.
B $\Phi \nvdash \psi$. Das ist die Widerspruchsannahme.

Wir führen einen neuen Begriff ein (*Konsistenz*) und argumentieren dann so:

1. Aus unser Widerspruchsannahme (B) folgt, dass $\Phi \cup \{\neg\psi\}$ konsistent sein muss.
2. Jede konsistente Menge hat ein Modell.
3. Hat $\Phi \cup \{\neg\psi\}$ ein Modell, so gilt $\Phi \not\models \psi$.
4. Dies ist dann ein Widerspruch zu (A).

8-18 ✎ Zur Übung

Zeigen Sie: Hat $\Phi \cup \{\neg\psi\}$ ein Modell, so gilt $\Phi \not\models \psi$.

8-19 Grundideen des Beweises in der Cocktail-Variante

Es gibt zwei Annahmen:

A Ihr Freundin kann Psi-Cocktails aus Φ mixen.
B Es gibt kein Anfängerrezept für Psi-Cocktails aus Φ.

Wir führen einen neuen Begriff ein (*Konsistenz*) und argumentieren dann so:

1. Aus unser Widerspruchsannahme (B) folgt, dass Φ zusammen mit Virgin-Psi konsistent sein muss.
2. Jede konsistente Menge hat ein Modell.
3. Hat Φ zusammen mit Virgin-Psi Modell, so gilt kann Ihre Freundin aus Φ keinen Psi-Cocktail mixen.
4. Dies ist dann ein Widerspruch zu (A).

8.3.3 Der Konsistenzbegriff

8-20 »Konsistenz« bedeutet, dass sich kein Quatsch ableiten lässt.

▶ Definition

Eine Menge Φ von Formeln heißt *konsistent*, wenn *nicht* $\Phi \vdash \neg(a \to a)$ gilt.
(»Man kann keinen Quatsch aus Φ ableiten.«)

Beispiele

- Die Menge $\{a, b\}$ ist konsistent.
- Die Menge $\{\neg(a \to a), b\}$ ist nicht konsistent.
- Die Menge $\{a, \neg a\}$ ist nicht konsistent.

Bemerkung: Statt $\neg(a \to a)$ könnte man jede beliebige Kontradiktion nutzen in der Definition.

8-21 ✎ Zur Übung

Zeigen Sie:

▶ Lemma

Ist Φ konsistent und gilt $\Phi \vdash \psi$, so ist auch $\Phi \cup \{\varphi\}$ konsistent.

▶ Lemma

Hat eine Menge Φ ein Modell, so ist sie konsistent.

(Unser Hauptziel im Rest des Kapitels ist, die Umkehrung zu zeigen: *Ist Φ konsistent, so hat Φ ein Modell.*)

8-22 Von der Widerspruchsannahme zur Konsistenz.

▶ Lemma

Falls $\Phi \nvdash \psi$, so ist $\Phi \cup \{\neg\psi\}$ konsistent.

Beweis. Nehmen wir an, $\Phi \cup \{\neg\psi\}$ wäre nicht konsistent.[1] Dann gilt

$$\Phi \cup \{\neg\psi\} \vdash \neg(a \to a)$$

und nach dem Deduktionstheorem somit

$$\Phi \vdash \neg\psi \to \neg(a \to a)$$

Nun gilt aber $\neg\psi \to \neg(a \to a) \vdash \psi$ nach Übung 8.1 und damit

$$\Phi \vdash \psi.$$

Widerspruch. □

Kommentare zum Beweis

[1] Schon wieder eine Widerspruchsannahme. Gut, dass es hier Lemmas gibt.

Konsistenz in der Cocktail-Variante. 8-23

Definition
Eine Menge Φ von Zutaten heißt *konsistent,* wenn es kein Anfängerrezept für den Negatoa-Cocktail gibt, das nur diese Zutaten nutzt.

Lemma
Falls es kein Anfängerrezept für den Psi-Cocktail mit Zutaten aus Φ gibt, so gibt es auch kein Anfängerrezept für den Negatoa-Cocktail aus Φ und Virgin-Psi $(\neg\psi)$.

Was wir alles schon erreicht haben. 8-24

Es gibt zwei Annahmen:
A $\Phi \models \psi$. Das war eine Voraussetzung im Satz.
B $\Phi \not\vdash \psi$. Das ist die Widerspruchsannahme.

Wir führen einen neuen Begriff ein (Konsistenz) und argumentieren dann so:
1. Aus unser Widerspruchsannahme (B) folgt, dass $\Phi \cup \{\neg\psi\}$ konsistent sein muss.
2. Jede konsistente Menge hat ein Modell.
3. Hat $\Phi \cup \{\neg\psi\}$ ein Modell, so gilt $\Phi \not\models \psi$.
4. Dies ist dann ein Widerspruch zu (A).

Was wir schon betreffend die Cocktails erreicht haben. 8-25

Es gibt zwei Annahmen:
A Ihr Freundin kann Psi-Cocktails aus Φ mixen.
B Es gibt kein Anfängerrezept für Psi-Cocktails aus Φ.

Wir führen einen neuen Begriff ein (Konsistenz) und argumentieren dann so:
1. Aus unser Widerspruchsannahme (B) folgt, dass Φ zusammen mit Virgin-Psi konsistent sein muss.
2. Jede konsistente Menge hat ein Modell.
3. Hat Φ zusammen mit Virgin-Psi Modell, so gilt kann Ihre Freundin aus Φ keinen Psi-Cocktail mixen.
4. Dies ist dann ein Widerspruch zu (A).

8.3.4 Jede konsistente Menge hat ein Modell

Vorbereitung des zentralen Satzes: Maximale Konsistenz. 8-26

Definition
Eine konsistent Menge Φ heißt *maximal konsistent,* wenn jede echte Obermenge von Φ inkonsistent ist.

(In der Cocktail-Variante: Eine Menge von Zutaten ist *maximal konsistent*, wenn es zwar kein Anfängerrezept für einen Negatoa-Cocktail mit ihnen gibt, aber *mit einer beliebigen weiteren Zutat schon*.)

Jede konsistente Menge lässt sich maximal erweitern. 8-27

Satz: Lindenbaum
Jede konsistente Menge hat eine maximal konsistente Obermenge.

(Beweisprinzip an Cocktails erklärt: Steht auf einem Tisch eine konsistent Menge an Zutaten, so betrachte *alle* möglichen weiteren Zutaten und stelle nacheinander immer eine weitere hinzu, solange die Menge nicht inkonsistent wird.)

Beweis. Sei Φ eine konsistente Menge.[1] Betrachte nun eine Aufzählung $\varphi_1, \varphi_2, \dots$ *aller* aussagenlogischen Formeln[2] und füge immer dann ein φ_i zu Φ hinzu, wenn die Menge konsistent bleibt. Formal: Sei $\Phi_0 = \Phi$ und sei $\Phi_{i+1} = \Phi_i \cup \{\varphi_{i+1}\}$, falls letzteres konsistent ist, sonst sei $\Phi_{i+1} = \Phi_i$.
Betrachte nun $\Phi' := \bigcup_{i=1}^{\infty} \Phi_i$.[3]
Offenbar ist Φ' eine Obermenge von Φ. Weiter ist Φ' maximal konsistent:
– Φ' ist konsistent, denn ein Beweis $\Phi \vdash \neg(a \to a)$ müsste *endlich viele Formeln* nutzen und somit nur Formeln aus Φ_i für ein hinreichend großes i. Damit wäre auch schon Φ_i inkonsistent, was aber nicht der Fall war.
– Φ' ist maximal, denn das Hinzufügen einer beliebigen nicht enthaltenen Formel φ_i machte Φ_{i-1} inkonsistent.

□

Kommentare zum Beweis
[1] Beweisrezept All-Aussagen beweisen
[2] Dass es die gibt, ist gar nicht so offensichtlich. Sehen Sie, warum es sie gibt?
[3] Beweisrezept Konstruktiver Beweis.

8-28 Der Hauptsatz: Jede konsistente Menge hat ein Modell.

▶ Satz
Jede konsistente Menge von aussagenlogischen Formeln hat ein Modell.

Der Beweis geht in folgenden Schritten:

1. Sei Φ die konsistente Menge.
2. Dann gibt es eine maximal konsistente Obermenge Φ' von Φ.
3. Sei β folgende Welt: Für eine Variable v sei $\beta(v) = 1$ genau dann, wenn $v \in \Phi'$.
4. Wir zeigen durch eine Induktion über den Aufbau, dass für jede Formel ρ gilt: $\hat{\beta}(\rho) = 1$ genau dann, wenn $\rho \in \Phi'$.
5. Damit ist β ein Modell von Φ' und damit auch von Φ.

8-29 Der einfachste Fall: Variablen.

▶ Lemma
Ist ρ eine Variable, so gilt $\hat{\beta}(\rho) = 1$ genau dann, wenn $\rho \in \Phi'$.

Beweis. So haben wir β definiert. □

8-30 Der etwas schwierigere Fall: Negationen.

▶ Lemma
Für ρ' gelte: $\hat{\beta}(\rho') = 1$ genau dann, wenn $\rho' \in \Phi'$.
Ist $\rho = \neg\rho'$, so gilt $\hat{\beta}(\rho) = 1$ genau dann, wenn $\rho \in \Phi'$.

Beweis. Offenbar gilt $\rho' \notin \Phi'$ genau dann, wenn $\hat{\beta}(\rho) = 0$. Da Φ' maximal konsistent ist, gilt $\neg\rho' \in \Phi'$ genau dann, wenn $\rho' \notin \Phi'$ (es können nicht beide in Φ' sein, aber es kann nicht schaden, eines hinzuzunehmen). Also gilt $\rho = \neg\rho' \in \Phi'$ genau dann, wenn $\hat{\beta}(\rho) = 1$. □

8-31 Der schwierige Fall: Implikationen.

▶ Lemma
Für ρ_1 und ρ_2 gelte: $\hat{\beta}(\rho_i) = 1$ genau dann, wenn $\rho_i \in \Phi'$.
Ist $\rho = \rho_1 \to \rho_2$, so gilt $\hat{\beta}(\rho) = 1$ genau dann, wenn $\rho \in \Phi'$.

Kommentare zum Beweis

[1] Beweisrezept Zwei Richtungen.

Beweis. Wir zeigen, dass $\rho \notin \Psi$ genau dann gilt, wenn $\hat{\beta}(\rho) = 0$. Dazu zeigen wir zwei Richtungen.[1]
Für die eine Richtung sei $\hat{\beta}(\rho) = 0$. Dann gelten $\hat{\beta}(\rho_1) = 1$ und $\hat{\beta}(\rho_2) = 0$. Dies bedeutet $\rho_1 \in \Phi'$ und $\rho_2 \notin \Phi'$. Wäre $\rho = \rho_1 \to \rho_2 \in \Phi'$, so müsste wegen der Abgeschlossenheit unter Ableitungen nun folgen $\rho_2 \in \Phi'$. Da dies nicht der Fall ist, schließen wir $\rho \notin \Phi'$.
Für die zweite Richtung sei nun $\rho \notin \Phi'$. Dann ist $\neg\rho \in \Phi'$ (dasselbe Argument wie weiter oben). Aus $\neg\rho$ kann man aber folgende Ableitungen bilden: $\{\neg(\rho_1 \to \rho_2)\} \vdash \rho_1$ und $\{\neg(\rho_1 \to \rho_2)\} \vdash \neg\rho_2$, da man direkt zeigen kann, dass gelten $\vdash \neg(\rho_1 \to \rho_2) \to \rho_1$ und auch $\vdash \neg(\rho_1 \to \rho_2) \to \neg\rho_2$, siehe Übungsaufgabe 8.2. Nach Voraussetzung ergibt dies $\hat{\beta}(\rho_1) = 1$ und $\hat{\beta}(\rho_2) = 0$, also $\hat{\beta}(\rho) = 0$. □

Zusammenfassung dieses Kapitels

8-32 ▶ »Hauptsatz« der Aussagenlogik
$\Phi \models \psi$ gilt genau dann, wenn $\Phi \vdash \psi$.

(Ihre Freundin kann aus Zutaten Φ genau dann einen Psi-Cocktail mixen, wenn es ein Anfängerrezept hierfür für Sie gibt.)

Übungen zu diesem Kapitel

Übung 8.1 Einen Hilbertbeweis führen, mittel

Zeigen Sie, dass es einen Hilbert-Beweis mit dem Axiomsystem von Mendelson dafür gibt, dass die Formel $(\neg b \to \neg(a \to a)) \to b$ eine Tautologie ist.

Tipps: Zeigen Sie mithilfe des Deduktionstheorems nacheinander folgendes »Sätze«:

1. $\{b\} \vdash a \to b$ (einfach Axiom I benutzen).
2. $\{b \to c\} \vdash a \to (b \to c)$ (vorherigen Satz benutzen).
3. $\{a \to b, b \to c\} \vdash a \to c$ (Axiom II und vorigen Satz benutzen).
4. $\{a \to (b \to a), (b \to a) \to c\} \vdash a \to c$ (vorigen Satz benutzen)
5. $\{(b \to a) \to c\} \vdash a \to c$ (vorigen Satz und Axiom I benutzen)
6. $\{(\neg b \to a) \to b\} \vdash a \to b$ (vorigen Satz benutzen)
7. $\{\neg b \to \neg a\} \vdash (\neg b \to a) \to b$ (Axiom III benutzen)
8. $\{\neg b \to \neg a\} \vdash a \to b$ (beide vorigend Sätze kombinieren).
9. $\{\neg b \to \neg(a \to a)\} \vdash (a \to a) \to b$ (vorigen Satz benutzen).
10. $\vdash a \to a$ (in Beispiel 7-13 gezeigt)
11. $\{\neg b \to \neg(a \to a)\} \vdash b$.

Übung 8.2 Einen Hilbertbeweis führen, schwer

Zeigen Sie, dass es einen Hilbert-Beweis mit dem Axiomsystem von Mendelson dafür gibt, dass die Formeln $\neg(\rho_1 \to \rho_2) \to \rho_1$ und auch $\neg(\rho_1 \to \rho_2) \to \neg\rho_2$ Tautologien sind.

Tipps: Benutzen Sie das Deduktionstheorem und zeigen Sie:

1. $\vdash (a \to b) \to (\neg b \to \neg a)$
2. $\vdash (\neg b \to \neg a) \to (a \to b)$
3. $\vdash a \to \neg\neg a$
4. $\vdash \neg\neg a \to a$

Übung 8.3 Axiomensystem von Frege, schwer

Statt dem Axiomensystem aus diesem Kapitel kann man auch nach anderen Systemen Ausschau halten. Das älteste System stammt von Frege aus dem Jahr 1879, auch wenn dieser dessen Vollständigkeit nicht zeigen konnte. Es lautet:

I $\varphi_1 \to (\varphi_2 \to \varphi_1)$
II $\big(\varphi_1 \to (\varphi_2 \to \varphi_3)\big) \to \big((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\big)$
III $(\varphi_1 \to (\varphi_2 \to \varphi_3)) \to (\varphi_2 \to (\varphi_1 \to \varphi_3))$
IV $(\varphi_1 \to \varphi_2) \to (\neg\varphi_2 \to \neg\varphi_1)$
V $\neg\neg\varphi_1 \to \varphi_1$
VI $\varphi_1 \to \neg\neg\varphi_1$

Zeigen Sie, dass dieses Axiomensystem korrekt und vollständig ist.

Tipp: Zeigen Sie für die Vollständigkeit, dass sich Axiom III aus Mendelsons System aus den obigen Regeln ableiten lässt.

Übung 8.4 Axiomensystem von Meredith, schwer

Verblüffenderweise gibt es ein vollständigs Axiomensystem der Aussagenlogik mit einem *einzigen* Axiom. Zeigen Sie, dass folgendes Axiomensystem von Meredith korrekt und vollständig ist:

I $((((\varphi_1 \to \varphi_2) \to (\neg\varphi_3 \to \neg\varphi_4)) \to \varphi_3) \to \varphi_5) \to ((\varphi_5 \to \varphi_1) \to (\varphi_4 \to \varphi_1))$

Teil IV
Prädikatenlogik

Die Prädikatenlogik ist die Königin unter den Logiken. Dies liegt nicht etwa daran, dass sie die komplizierteste Logik ist (es gibt Logiken mit wesentlich komplexerer Syntax und Semantik), sondern daran, dass sich schlichtweg *die gesamte Mathematik* in ihr ausdrücken lässt. Jeder wahre mathematische Sachverhalt, vom epochalen Fundamentalsatz über gewöhnliche Feld-Wald-und-Wiesen-Sätze bis zur unbedeutendsten Nebenhilfsuntersonderbeobachtung, lässt sich als prädikatenlogische Formel hinschreiben und auch in einem geeigneten Beweissystem beweisen.

Natürlich hat diese große Mächtigkeit der Prädikatenlogik ihren Preis:

1. Sowohl die Syntax wie die Semantik der Prädikatenlogik sind wesentlich komplexer als die der Aussagenlogik. Insbesondere für die Semantik werden wir einige völlig neue, teils recht technische Konzepte benötigen.
2. Es ist *viel* schwieriger herauszufinden, ob eine prädikatenlogische Formel eine Tautologie darstellt oder nicht. Dies war bei der Aussagenlogik zwar auch nicht einfach, aber letztendlich war es nur eine Frage, wie lange man bereit ist, auf eine Antwort zu warten. In den Veranstaltungen höherer Semester werden Sie noch lernen, dass es *unmöglich* ist, prädikatenlogische Tautologien auch mit beliebig viel Rechenzeit maschinell allgemein zu bestimmen.

Was sind nun aber die ominösen »Prädikate«, die der Logik ihren Namen geben? Sollten Sie ein Weinkennern sein, kennen Sie vielleicht den Begriff *Kabinettwein mit Prädikat*. Bevorzugen Sie handfesteres, so ist Ihnen vielleicht *Prädikats-Blutwurst* geläufig? Nein? Achten Sie beim nächsten Besuch des Fleischers Ihres Vertrauens darauf. In jedem Fall geht es bei einem Prädikat darum, unter der großen Menge aller Weine oder aller Blutwürste bestimmte *auszuzeichnen*, ihnen also ein besonderes Prädikat zu verleihen. Übersetzt man dieses Bild in die nüchterne Sprache der Mathematik, so bleibt leider nur eine wenig poetische Menge W von Weinen übrig und eine Menge $P \subseteq W$ von Weinen, die ein Prädikat haben. Es gilt dann $x \in P$ genau dann, wenn x ein Prädikatswein ist.

In der Prädikatenlogik werden wir auf der semantischen Seite verschiedene Prädikate haben, über die wir dann syntaktisch mittels Formeln reden. Beispielsweise besagt dann die Formeln $\exists x(P(x))$, dass es in der Welt mindestens einen Wein mit Prädikat gibt. Zum Wohl.

9-1

Kapitel 9
Syntax der Prädikatenlogik
Die Seifenoperlogik

9-2

Lernziele dieses Kapitels

1. Die geänderte Bedeutung von Variablen verstehen
2. Die Begriffe Relationssymbol, Quantor, Bindung, Signatur und Formel kennen und anwenden können
3. Natürlichsprachliche Problemstellungen prädikatenlogisch formulieren können

Inhalte dieses Kapitels

Worum es heute geht

In diesem und in den folgenden Kapiteln wird es um die *Prädikatenlogik* gehen. Schon das Wort ist deutlich einschüchternder als »Aussagenlogik« es war, die Anzahl der griechischen Silben ist beängstigend angestiegen. Hier deshalb ein Vorschlag für eine freundlichere Bezeichnung dieser Logik: *Seifenoperlogik*.

Bei der Prädikatenlogik geht es fast ausschließlich um die Frage, wer etwas mit wem hat, sich von wem getrennt hat, sich mit wem wieder vertragen hat, wer wen betrogen hat und wer böse ist, wer süß ist und wer hoffentlich nächste Folge nicht mehr dabei sein wird. Kurz, in der Prädikatenlogik geht es um *Beziehungen*. Beispielsweise können zwei Leute eine Beziehung haben, oder eben auch nicht. (In Wirklichkeit gibt es natürlich unendlich viele Zwischenstufen, aber die Wirklichkeit ignorieren wir wie üblich.) Es gibt auch verschiedene Arten von Beziehungen, so könnten zwei Leute in der Beziehung »wohnen zusammen« stehen, aber nicht in der Beziehung »lieben einander«. Bei manchen Beziehungen ist auch die »Richtung« wichtig: »Frau Müller-Lüdenscheid liebt Herrn Graf von Bruckelberger« ist etwas anderes als »Herr Graf von Bruckelberger liebt Frau Müller-Lüdenscheid«. Alle solche Beziehungen, bei denen zwei Personen beteiligt sind, werden wir etwas vornehmer *zweistellig* nennen. Im Rahmen einer Ménage à trois können auch drei Personen eine Beziehung unterhalten – oder eben auch nicht. Man spricht dann, wenig verwunderlich, von einer *dreistelligen* Beziehung. Wie im wirklichen Leben auch sind dreistellige Beziehungen allerdings seltener als zweistellige.

Wenn es zweistellige, dreistellige und natürlich auch vier- und fünfstellige Beziehungen gibt, dann erscheint es nur folgerichtig, dass es auch »einstellige Beziehungen« geben sollte. Statt auf ein Paar von Leuten trifft eine solche Beziehung nur auf eine einzelne Person zu – oder eben auch nicht. Hier von einer Beziehung zu sprechen ist allerdings reichlich unnatürlich, weshalb wir treffender das schöne Wort *Prädikat* benutzen werden. Beispiele von Prädikaten, die auf Leute zutreffen, sind »ist gemein« oder »mag Fische« oder »hat schwarze Haare«.

In der Seifenoperlogik geht es nun darum, komplexe Beziehungsgeflechte syntaktisch aufzuschreiben und dann semantisch auf ihre Korrektheit zu überprüfen. Um die Semantik wird es in späteren Kapiteln gehen, wir kümmern uns in diesem Kapitel zunächst um die Syntax.

Wie sollte man den Umstand »x hat was mit y und y hat was mit z« aufschreiben? Um so etwas schön knapp hinzuschreiben, werden wir »hat was mit« abkürzen durch, beispielsweise, ein »H«. Wer hier etwas mit wem hat, schreibt man in Klammern hinter den Buchstaben, also »$H(x,y)$ und $H(y,z)$«. Wie man das Wörtchen »und« los wird, wissen Sie natürlich schon, so dass wir »$H(x,y) \wedge H(y,z)$« als *prädikatenlogische Formel* erhalten. Nachteilig ist allerdings anzumerken, dass in der Formulierung $H(x,y) \wedge H(y,z)$ das große Drama etwas abhanden gekommen ist, das »x hat was mit y und y hat was mit z« noch innewohnte und Stoff für mehrere Seifenopernfolgen geboten hätte.

9.1 Motivation zur Prädikatenlogik

9.1.1 Grenzen der Aussagenlogik

9-4 **Die Aussagenlogik und die Gesundheitskarte.**

Copyright Bundesministerium für Gesundheit

Wir wollen Problemstellungen, die mit der Gesundheitskarte zusammenhängen, logisch formulieren. Die *Aussagenlogik kann helfen*, wenn man herausfinden möchte, ob Sätze war sind wie

- »Wenn die Karte in den Leser eingegeben wird und die PIN falsch eingegeben wurde, dann wird keine Verbindung hergestellt.«

Bei vielen Aussagen *hilft sie aber nicht weiter*, wie zum Beispiel:

- »Alle Leute, die eine bestimmte Krankheit haben, bekommen ein bestimmtes Medikament.«
- »Es gibt mindestens drei Personen mit Krankheit A, die kein passendes Medikament bekommen und trotzdem gesund wurden.«

9-5 **Die Aussagenlogik und die Peano-Arithmetik.**

Unknown author, public domain

In der Mathematik wollen wir über Zahlen und das Rechnen reden. Die *Aussagenlogik kann helfen*, wenn man herausfinden möchte, ob Sätze war sind wie

- »Wenn eine Zahl gerade ist, dann ist sie nicht ungerade.«

Bei vielen Aussagen *hilft sie aber nicht weiter*, wie zum Beispiel:

- »Es gibt eine Zahl, die nicht Summe zweier Primzahlen ist.«
- »Für alle Zahlen $n \geq 3$ gilt, dass es keine Zahlen $a,b,c > 1$ gibt mit $a^n + b^n = c^n$.«

9.1.2 Was ist Prädikatenlogik?

9-6 **Mögliche Erweiterungen der Aussagenlogik.**

Wir müssen die Aussagenlogik *erweitern*. Dies kann *nicht nur syntaktisch* passieren, wir wollen auch *über* neue Dinge reden können. Es gibt viele Möglichkeiten, wie man die Aussagenlogik erweitert (gerne auch kombiniert):

Temporallogik Durch syntaktische und semantische Elemente zur Beschreibung von *Zeit*.
»*Bevor* die Lampe leuchtet, muss jemand den Schalter gedrückt haben.«

Modallogik Durch syntaktische und semantische Elemente zur Beschreibung von *Notwendigkeit*.
»Es ist *möglich* aber *nicht notwendig*, dass es im Winter schneit.«

Prädikatenlogik Durch syntaktische und semantische Elemente zur Beschreibung von *Objekten und Eigenschaften*.
»Es gibt *jemanden*, der *krank* ist und nicht *behandelt* wird.«

9-7 **Prädikatenlogik – ein Überblick.**

Die *Prädikatenlogik* beschäftigt sich mit *Objekten* und *Aussagen* über deren *Eigenschaften*. Genau wie die Aussagenlogik hat sie eine *Syntax* und eine *Semantik*. Sie ist die *wichtigste Logik* in der Mathematik, da sich mit ihr die Mengenlehre und damit die *gesamte Mathematik* beschreiben lässt.
In der *Informatik* kommt sie vor allem in Spezifikationen vor.

9.2 Syntax der Prädikatenlogik

Rückblick: Die Sprache der Aussagenlogik. 9-8

Die *Syntax der Aussagenlogik* ist eine *Sprache* $L_{\text{Aussagenlogik}}$, die alle *Formeln der Aussagenlogik* enthält. Sie ist wie folgt aufgebaut:

- Es gibt *atomare Formeln*. Dies sind die Aussagenvariablen und die Sondersymbole `w` und `f`.
- Die atomaren Formeln lassen sich mittels Junktoren verknüpfen.

Formeln sind Wörter!

Die Prädikatenlogik übernimmt, verändert und erweitert die Syntax der Aussagenlogik. 9-9

Was gleich bleibt:

- Alle Junktoren wie $\wedge$ und $\rightarrow$ werden übernommen.
- Alle Formeln lassen sich eindeutig parsen.

Was sich ändert:

- Variablen stehen nicht mehr für wahr oder falsch, sondern für Objekte.
- Variablen sind keine atomare Formeln mehr.

Was neu ist:

- Es gibt Symbole für Prädikate.
- Es gibt die Quantoren $\forall$ und $\exists$.

9.2.1 Variablen und Relationssymbole

In der Prädikatenlogik stehen Variablen für Objekte. 9-10

In der Prädikatenlogik *stehen Variablen immer für Objekte*, niemals für Aussagen. *Objekte* können alles mögliche sein:

- Zahlen
- Medikamente
- Programme

Welche Objekte möglich sind, hängt von der *Welt* ab – dazu mehr, wenn wir die Semantik besprechen.

▶ **Definition:** Variablen in prädikatenlogischen Formeln

Eine *(prädikatenlogische) Variable* ist ein Wort der Form x, x', x'' und so weiter.

Zur Vereinfachung der Schreibweise benutzen wir auch andere Kleinbuchstaben außer x als Variablen wie y oder z' oder p_5.

Beispiel eines Textes und der darin vorkommenden Variablen. 9-11

Beispiel: Ein Text

Alle *Menschen* haben eine *Mutter* und einen *Vater*.

In diesem Text geht es um drei Objekte, für die man Variablen einführen kann:

- Es ist von einem (nicht näher bestimmten) »Mensch« die Rede. Für dieses Objekt könnten wir die Variable x verwenden.
- Es ist von einer (nicht näher bestimmten) »Mutter« und einem »Vater« die Rede. Für diese könnten wir die Variablen x' und x'' verwenden.

Beispiel: Text mit Variablen

Für alle x gibt ein x' und ein x'', so dass x' die Mutter und x'' der Vater von x sind.

9-12 **Relationssymbole stehen für Beziehungen und Eigenschaften.**
Ein *Relationssymbol* steht für Beziehungen zwischen Objekten oder die Eigenschaften von Objekten.

Beispiel: Ein Text
Alle Menschen *haben* eine Mutter und einen Vater.

- »Mutter sein« ist eine Eigenschaft, die ein Objekt (ein Mensch) haben kann (oder auch nicht).
- Auch »als Elternteil haben« ist eine Beziehung, die zwischen zwei Objekten (einem Menschen und einem anderen Menschen) bestehen kann.
- Für jede Eigenschaft und Beziehung gibt es ein *Relationssymbol*.
- Wir benutzen hierfür *Großbuchstaben*: M für »Mutter sein«, V für »Vater sein«, H für »als Elternteil haben«.

9.2.2 Atomare Formeln

9-13 **Die zwei Arten von atomaren Formeln.**
Anders als in der Aussagenlogik sind *atomare Formeln* keine Variablen, sondern werden wie folgt gebildet:

Definition: Atomare Formeln
Eine *atomare Formel* ist ein Wort von einer folgender Formen:

1. ein Relationssymbol gefolgt von Variablen in Klammern oder
2. zwei Variablen mit einem $=$ dazwischen.

Beispiel: $M(x')$ oder $V(x'')$ oder $H(x,x')$ oder $x=x$ oder $x'''=x'$

Eine atomare Formel ist *wahr oder falsch*, je nachdem, ob die Beziehung zwischen den Objekten besteht; beziehungsweise, ob die Variablen dasselbe Objekt bezeichnen. Wieder *hängt es von der Welt ab* was der Fall ist – dazu mehr, wenn mir die Semantik besprechen.

9-14 **Teil-Übersetzung des Textes in eine Formel.**

Beispiel: Ein Text
Alle Menschen haben eine Mutter und einen Vater.

Teile des Textes lassen sich nun mit atomaren Formeln schreiben:

Beispiel: Ersetzung der atomaren Formeln
Für alle x gibt ein x' und ein x'', so dass $M(x')$ und $V(x'')$ und $H(x,x')$ und $H(x,x'')$.

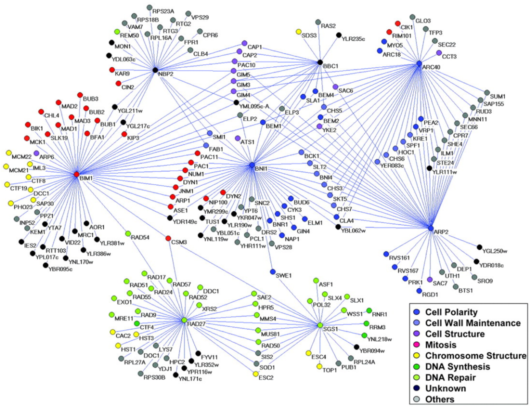
9-15 **Verknüpfung von Formeln mit Junktoren.**
Genau wie in der Aussagenlogik kann man atomare Formeln mit Junktoren verknüpfen.

Beispiel: Ein Text
Alle Menschen haben eine Mutter und einen Vater.

Beispiel: Verknüpfung mittels Junktoren
Für alle x gibt ein x' und ein x'', so dass $M(x') \wedge V(x'') \wedge H(x,x') \wedge H(x,x'')$.

9.2.3 Signaturen

✎ Zur Diskussion: Welche Relationssymbole erscheinen sinnvoll? 9-16



Literatur

[1] A. H. Y. Tong, E. Evangelista, A. P. Parsons et al. Systematic Genetic Analysis with Ordered Arrays of Yeast Deletion Mutants, *Science,* 294(5550):2364–2368, 2001.

Beobachtung: Die Menge der Relationssymbole hängt vom Kontext ab. 9-17

Die Menge der (sinnvollen) Relationssymbole hängt vom *Kontext* ab beziehungsweise davon, was *spezifiziert werden soll*. Deshalb werden wir die Relationssymbole, die wir benutzen wollen, *deklarieren* mittels einer *Signatur*.
Bemerkung: Ähnlich wie in der Programmierung sind Deklarationen *nicht wirklich nötig*, haben sich aber als *sehr praktisch* erwiesen.

Definition und Schreibweise für Signaturen. 9-18

▶ Definition

Eine *(relationale) logische Signatur* besteht aus einer Menge von *Relationssymbolen* und einer Abbildung, die jedem dieser Relationssymbole eine *Stelligkeit* zuordnet.

Notationen

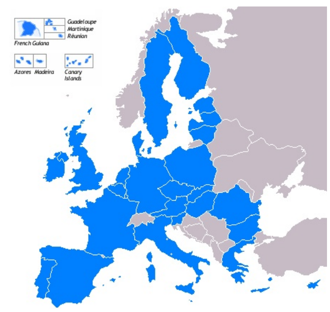
- Wir benutzen kleine griechische Buchstaben für Signaturen (meist σ oder τ).
- Signaturen schreibt man auf, indem man die Menge der Relationssymbole als Liste in runden Klammern aufschreibt.
- Die Stelligkeit der Relationssymbole schreibt man als hochgestellte Indizes an die Relationssymbole.

Beispiel

Die Signatur $\tau = (E^2, P^1, R^1)$ enthält drei Relationssymbole, nämlich E, P und R. Die Stelligkeit von E ist 2, die von P und R ist jeweils 1.

✎ Zur Übung 9-19

Das Vier-Farben-Problem ist die Frage, ob sich jede Landkarte mit vier Farben färben lässt, so dass nebeneinanderliegende Länder unterschiedliche Farben haben.
Die »Dinge« sind nun Länder, es besteht eine »Liegen-Nebeneinander-Beziehung« zwischen Ländern und es gibt vier Prädikate für die Färbung von Ländern.
Geben Sie die Signatur an.



9.2.4 Quantoren und Bindung

9-20 Quantoren zählen Objekte und binden Variablen.

Mit einem *Quantor* kann man eine Formel bauen, die eine Behauptung über die *Anzahl* an Objekte mit einer *Eigenschaft* macht. Diese Eigenschaft ist dabei durch eine Formel gegeben.

Beispiel: Ein Text

Alle Menschen haben eine Mutter und einen Vater.

Beispiel: Quantifizierung über die Anzahl der Personen

$\forall x\bigl(\exists x'\bigl(\exists x''\bigl(M(x') \wedge V(x'') \wedge H(x,x') \wedge H(x,x'')\bigr)\bigr)\bigr).$

9-21 Syntax von Quantoren

▶ Definition: Formel mit Quantoren

Ist das Wort φ eine prädikatenlogische Formel und v eine Variable, so sind auch folgende Wörter prädikatenlogische Formeln:

- $\forall v(\varphi)$
- $\exists v(\varphi)$

- Die Formel $\forall v(\varphi)$ ist *wahr oder falsch*, je nachdem, ob für alle möglichen v die Formel φ wahr ist.
- Die Formel $\exists v(\varphi)$ ist *wahr oder falsch*, je nachdem, ob für wenigstens ein v die Formel φ wahr ist.
- Wieder *hängt es von der Welt ab*, was los ist – dazu mehr, wenn wir die Semantik besprechen.

9-22 Verdecken von Variablen in Programmen.

```
static int foo (int x)
{
  int y = 5;
  x = y;
  y++;
  {
    int x = 10;
    y = x;
    x = 5;
  }
  x = y;

  return x;
  // Welcher Wert wird zurückgegeben?
}
```

9-23 Quantoren binden Variablen

In einer Formel wie $\forall x(L(x,y))$ ist *x durch den Quantor gebunden*, wohingegen *y frei ist*. Die durch eine Quantor gebundene Variable *funktioniert sehr ähnlich wie ein lokale Variable in Java*:

- Die Variable x ist in $\forall x(\varphi)$ nur innerhalb von φ gebunden.
- Hat x außerhalb der Teilformel bereits einen Wert, so wird dieser *verdeckt*.
- Wird eine Variable mehrfach gebunden, so ist immer nur der Wert aus der innersten Bindung sichtbar.

In einer Formel wie $x = x \wedge \forall x(x = y)$ ist *x sowohl frei als auch gebunden*.

Definition von freien und gebundenen Variablen. 9-24

▶ **Definition**
Sei φ eine prädikatenlogische Formel. Die Mengen $\text{free}(\varphi)$ und $\text{bound}(\varphi)$ sind wie folgt definiert:

1. Ist φ eine atomare Formel, so ist $\text{free}(\varphi)$ die Menge der in φ vorkommenden Variablen und $\text{bound}(\varphi)$ ist leer.
2. Ist $\varphi = \neg\psi$, so ist $\text{free}(\varphi) = \text{free}(\psi)$ und ebenso $\text{bound}(\varphi) = \text{bound}(\psi)$.
3. Ist $\varphi = \psi \circ \rho$, wobei $\circ$ ein Junktor ist, so ist $\text{free}(\varphi) = \text{free}(\psi) \cup \text{free}(\rho)$ und ebenso $\text{bound}(\varphi) = \text{bound}(\psi) \cup \text{bound}(\rho)$.
4. Ist $\varphi = \exists v(\psi)$ oder $\varphi = \forall v(\psi)$, so ist $\text{free}(\varphi) = \text{free}(\psi) \setminus \{v\}$ und weiter $\text{bound}(\varphi) = \text{bound}(\psi) \cup \{v\}$.

Eine Formel ohne freie Variablen heißt *geschlossen*.

✎ **Zur Übung** 9-25
Bestimmen Sie die gebundenen und die freien Variablen der folgenden Formel:

$$\forall x\big(V(x,y) \to T(x)\big) \wedge \exists y\Big(\forall z\big(V(x,y)\big) \to T(x)\Big).$$

Zusammenfassung dieses Kapitels

▶ **Logische Signatur (vorläufig)** 9-26
Eine *(logische) Signatur* besteht aus Relationssymbolen und einer Funktion, die jedem Relationssymbol eine positive natürliche Zahl zuordnet, die *Stelligkeit* genannt.

▶ **Beispiel einer logischen Signatur**
$\tau = (N^2, R^1, G^1, B^1, Y^1)$.

▶ **Syntax von prädikatenlogischen Formeln (vorläufig)**
Sei σ eine Signatur. Die *prädikatenlogischen Formeln* zu dieser Signatur sind Wörter über dem Alphabet $\{x, {}', (,), \forall, \exists, \wedge, \vee, \to, \leftrightarrow, =, \text{Kommasymbol}\} \cup R$, wobei R die Mengen der Relationssymbole in σ ist. Folgende Wörter sind *atomare Formeln*:

1. $u = v$, wobei u und v von der Form $x'^{\cdots\prime}$ sind, oder
2. $R(v_1, \dots, v_n)$, wobei R ein n-stelliges Relationssymbol ist und die v_i von der Form $x'^{\cdots\prime}$ sind.

Neben den atomaren Formeln sind weiterhin folgende Wörter Formeln:

3. $\neg\varphi$, wenn φ bereits eine Formel ist.
4. $(\varphi \circ \psi)$, wenn $\circ$ einer der Junktoren $\wedge$, $\vee$, $\to$ oder $\leftrightarrow$ ist und φ und ψ Formeln sind.
5. $\exists v(\varphi)$ und auch $\forall v(\varphi)$, wenn v eine Variable ist und φ eine Formel.

Übungen zu diesem Kapitel

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

5 min Prüfungsfrage 9.1 → Lösung

Bindungen bestimmen

Geben Sie für folgende Formeln die gebundenen und freien Variablen an.

1. $Q(x, f(h(y))) \vee \forall x(P(x,x,x))$
2. $\exists y \forall x \exists z(f(x) = g(y) \vee \neg R(1,z,f(x)))$
3. $\forall x(f(x) = g(y) \vee \exists y(R(x,h(x))))$
4. $\exists z(Q(y) \vee P(z)) \wedge \exists y(Q(z) \vee f(z) = g(z))$

8 min Prüfungsfrage 9.2 → Lösung

Formeln analysieren

Geben Sie für folgende Formeln an, ob es sich um aussagenlogische oder prädikatenlogische Formeln handelt und welche Variablen, Junktoren, Relationssymbole vorkommen.

1. $Q(a) \vee P(x)$
2. $\forall x(P(x,s) \to R(a))$
3. $a \vee (b \to (a \wedge \neg c))$
4. $\exists x(\forall y(h(f(x),x) = g(y)))$

10 min Prüfungsfrage 9.3 → Lösung

Grammatik für die Syntax

Geben Sie eine Grammatik für die Prädikatenlogik an, wobei folgende Besonderheiten zu beachten sind:

1. Die Signatur lautet $\sigma = (S^1)$.
2. Als einzige Junktoren sind $\neg$ und $\wedge$ zugelassen.

Geben Sie neben den Regeln explizit die Menge der Terminalsymbole Ihrer Grammatik an, sowie die Menge der Nonterminalsymbole und auch das Startsymbol.

6 min Prüfungsfrage 9.4

Bindungen bestimmen

Geben Sie bei folgenden Formeln jeweils die frei vorkommenden und die gebundenen Variablen an.

1. $\forall x \exists y \forall z(P(x,y) \vee Q(z))$
2. $P(x) \vee \neg(Q(y,v) \to f(x) = f(y))$
3. $P(x, f(y)) \vee \exists z(g(x,z) = f(y))$
4. $\forall x \exists y(P(x) \vee \neg Q(g(y))) \leftrightarrow (P(y) \wedge Q(x))$

10 min Prüfungsfrage 9.5

Texte formalisieren

Unendliche Weiten, Episode 5: First Contact

Captain Archer und Sub-Commander T'Pol beamen nach einer ersten Kontaktaufnahme mit den Bewohnern des Planeten Zwe wieder zurück auf die Enterprise und haben Folgendes zu berichten:

1. *Es gibt nur Zwillingsgeburten, wobei Zwillinge grundsätzlich verschiedenen Geschlechts sind. (Es gibt auch auf Zwe nur zwei Geschlechter. Außerdem ist niemand Zwilling von sich selbst.)*
2. *Die Bewohner essen niemals allein.*
3. *Zwillinge essen niemals zusammen.*

Übersetzen Sie die drei Aussagen in eine prädikatenlogische Formel F, wobei die ausschließliche Geburt von Zwillingen so zu interpretieren ist, dass jeder Bewohner genau einen Zwillingsbruder oder eine Zwillingsschwester hat. Die Sätze in Klammern sollen nicht übersetzt werden.

(Diese Aufgabe ist dem Buch *Logik für Informatiker* von Martin Kreuzer und Stefan Kühling entnommen.)

10 min Prüfungsfrage 9.6

Texte formalisieren

Unendliche Weiten, Episode 5: First Contact

Captain Archer und Sub-Commander T'Pol beamen nach einer ersten Kontaktaufnahme mit den Bewohnern des Planeten Zwe wieder zurück auf die Enterprise und haben Folgendes zu berichten:

1. *Es gibt nur Zwillingsgeburten, wobei Zwillinge grundsätzlich verschiedenen Geschlechts sind. (Es gibt auch auf Zwe nur zwei Geschlechter. Außerdem ist niemand Zwilling von sich selbst.)*
2. *Die Bewohner essen niemals allein.*
3. *Zwillinge essen niemals zusammen.*

Übersetzen Sie die drei Aussagen in eine prädikatenlogische Formel F, wobei die ausschließliche Geburt von Zwillingen so zu interpretieren ist, dass jeder Bewohner genau einen Zwillingsbruder oder eine Zwillingsschwester hat. Die Sätze in Klammern sollen nicht übersetzt werden.

(Diese Aufgabe ist dem Buch *Logik für Informatiker* von Martin Kreuzer und Stefan Kühling entnommen.)

Lösung zu 9.1

1. Formel: $Q(x, f(h(y))) \vee \forall x(P(x,x,x))$
   Gebundene Variablen: x
   Freie Variablen: x, y
2. Formel: $\exists y \forall x \exists z(f(x) = g(y) \vee \neg R(1,z,f(x)))$
   Gebundene Variablen: x, y, z
   Freie Variablen: keine
3. Formel: $\forall x(f(x) = g(y) \vee \exists y(R(x,h(x))))$
   Gebundene Variablen: x, y
   Freie Variablen: y
4. Formel: $\exists z(Q(y) \vee P(z)) \wedge \exists y(Q(z) \vee f(z) = g(z))$
   Gebundene Variablen: y, z
   Freie Variablen: y, z

Lösung zu 9.2

1. $Q(a) \vee P(x)$ ist eine prädikatenlogische Formel.
   Variablen: a, x.
   Junktoren: $\vee$.
   Relationssymbole: Q, R.
   Funktionssymbole: keine.
2. $\forall x(P(x,s) \to R(a))$ ist eine prädikatenlogische Formel.
   Variablen: x, s, a.
   Junktoren: $\to$.
   Relationssymbole: P, R.
   Funktionssymbole: keine.
3. $a \vee (b \to (a \wedge \neg c))$ ist eine aussagenlogische Formel.
   Variablen: a, b, c.
   Junktoren: $\vee$, $\to$, $\wedge$, $\neg$.
   Relationssymbole: keine.
   Funktionssymbole: keine.

4. $\exists x(\forall y(h(f(x),x) = g(y)))$ ist eine prädikatenlogische Formel.
   Variablen: x, y.
   Junktoren: keine.
   Relationssymbole: keine.
   Funktionssymbole: h, f, g.

Lösung zu 9.3

- Die Menge der Terminale ist $\{\forall, \exists, x, {}', (,), \wedge, \neg, S, =\}$.
- Die Menge der Nonterminale sind die Symbole F (für »Formel«), A (für »atomare Formel«) und V (für »Variable«).
- Das Startsymbol ist F.
- Die Regeln sind:

$$
\begin{aligned}
&F \to A \mid \forall V(F) \mid \exists V(F) \mid \neg F \mid (F \wedge F)\\
&A \to V = V \mid S(V)\\
&V \to x \mid V'
\end{aligned}
$$

10-1

Kapitel 10

Semantik der Prädikatenlogik

$\forall x(\exists y(hatteSexMit(x,y)))$ oder $\exists x(\forall y(hatteSexMit(x,y)))$?

10-2

Lernziele dieses Kapitels

1. Grundidee der relationalen Datenbank kennen
2. Den Begriff der relationalen logischen Struktur verstehen
3. Den Begriff der prädikatenlogischen Welt verstehen
4. Prädikatenlogische Begriffe Modell, Tautologie, Kontradiktion und Erfüllbarkeit kennen und anwenden können

Inhalte dieses Kapitels

Worum es heute geht

In der Einleitung zum vorherigen Kapitel wurde bereits ebenso scharfsinnig wie überzeugend argumentiert, dass die Prädikatenlogik besser Seifenoperlogik heißen sollte. Die Syntax der Prädikatenlogik ist eigentlich nur eine Methode, Umstände wie »x hat was mit y und y hat was mit z« knapper aufzuschreiben als »$H(x,y) \wedge H(y,z)$«.

Was *bedeutet* nun aber $H(x,y) \wedge H(y,z)$? Sprich: was ist die Semantik einer solchen Formel? Man könnte ganz einfach antworten: »Na, das bedeutet natürlich, dass x was mit y hat und y was mit z hat.« Jedoch ist das noch nicht wirklich hilfreich, denn wer ist denn dieser Mr. x? Und wer ist y? Und was bedeutet eigentlich »hat was mit«? Im Rahmen von *Sex and the City* bedeutet das sicherlich etwas anderes als im Rahmen der *Teletubbies*. Die Sachlage ist also komplizierter als bei der Aussagenlogik, wo man für jede Variable einfach festlegen musste, ob sie wahr oder falsch war, und schon hatte man eine Welt.

In der Seifenoperlogik legt eine Welt alles fest, was nötig ist, um einer Formel wie $H(x,y) \wedge H(y,z)$ einen Sinn einzuhauchen. Ausgangspunkt ist der Cast der Seifenoper, also die Personen, die alle mitspielen. Diese sind diejenigen, die als Mr. x oder Mrs. y in Frage kommen. Großspurig wird diese Menge an Personen in der Logik *Universum* genannt, der Begriff ist wohl etwas überdimensioniert geraten – aber wie so oft kann man ihn nicht mehr ändern. Als nächstes muss man festlegen, wer in einer Welt hinter den Variablen steckt, beispielsweise könnte Mr. X gerade John Preston sein, Mrs. Y gerade Carrie Bradshaw. Da es sich fürchterlich unwissenschaftlich anhören würde, spräche man immer von »der Filmfigur, die hinter Mr. x steckt«, benutzt man in der Logik lieber »das Element $\alpha(x)$ des Universum, das die Variablenbelegung α der Variable x zuordnet« – gemeint ist aber dasselbe. Schließlich muss man noch festlegen, was genau mit einer Formulierung wie »hat etwas mit« beziehungsweise mit »H« gemeint ist.

Durch diese ganzen Festlegungen entsteht am Ende die »Welt« *Sex and the City*. Die »Welt« der *Teletubbies* hingegen hat andere Charaktere, eine andere Bedeutung der Variablen, andere Beziehungen zwischen den Charakteren; jedoch kann man sich trotzdem genauso fragen, ob die Formel $H(x,y) \wedge H(y,z)$ in der Teletubbies-Welt gilt.

In diesem Kapitel wird es hautsächlich darum gehen, den Sprung von den doch recht anschaulichen (im wahrsten Sinne des Wortes) Seifenopern zu ihren mathematischen Formalisierungen zu schaffen. Wie immer ist dies nicht ganz leicht, aber wie immer macht auch hier Übung den Meister.

10.1 Relationen

10.1.1 Relationale Datenbanken

Eine Datenbank für die Gesundheitskarte. 10-4

Copyright Bundesministerium für Gesundheit

Ein Gesetz legt fest, dass Anfang 2006 in Deutschland die *elektronische Gesundheitskarte* eingeführt wird. Sie ist *eine Art Schlüssel, um auf eine große Datenbank zuzugreifen*. Die verbreitetste Art von Datenbanken sind *relationale* Datenbanken. Wie der Name schon sagt, speichern diese *ausschließlich Relationen (=Tabellen)* – dies aber sehr effizient.

Eigenschaften von Tabellen in einer relationalen Datenbank

- Jede Tabelle hat einen *eindeutigen Namen*.
- Die *Spalten* können auch *Namen haben* und ihre Anzahl ist für jede Tabelle fest.
- Jede *Zeile* repräsentiert einen Datensatz. Die Anzahl der Zeilen ist *veränderlich*.

Zwei Datenbanktabellen für das Gesundheitswesens. 10-5

Beispiel: Tabelle `Medikamente`

Produkt	Wirkstoff	zugelassen
Aspirin	Acetylsalicylsäure	ja
Homöofix	keiner	ja
Zinkofix	Zink	ja

Beispiel: Tabelle `wirkt_gegen`

Wirkstoff	Krankheit
Acetylsalicylsäure	Kopfschmerzen
Acetylsalicylsäure	Entzündungen
Zink	Zinkmangel

Man kommuniziert mittels SQL mit einer Datenbank. 10-6

Es gibt eine *einheitliche Sprache*, genannt SQL (Structured Query Language), um mit einer Datenbank zu »kommunizieren«. In dieser Sprache gibt Befehle, um Tabellen anzulegen, Daten in Tabellen einfügen, zu löschen und zu verändern. Mit dem wichtigsten Befehl, dem `select`*-Befehl*, kann man sich Tabellen *anschauen* und *Tabellen kombinieren*.

Beispiel

```
mysql> select * from medikamente;
+-----------+---------------------+------------+
| produkt   | wirkstoff           | zugelassen |
+-----------+---------------------+------------+
| Aspirin   | Acetylsalicylsaeure | true       |
| Homoeofix | null                | true       |
| Zinkofix  | Zink                | true       |
+-----------+---------------------+------------+
```

10.1.2 Relationen mathematisch

10-7 **Tabelle = Relation.**

Tabellen sind mathematisch *Relationen*:

Definition: Relation

Seien A_1 bis A_n Mengen. Eine *Relation* auf diesen Mengen ist eine Teilmenge von $A_1 \times \cdots \times A_n$.

Bemerkungen: Das *Kreuzprodukt* $A_1 \times \cdots \times A_n$ enthält gerade alle Tupel, deren erste Komponente aus A_1 stammt, deren zweites Komponente aus A_2 und so weiter. Eine *Teilmenge* dieses Kreuzprodukt ist also eine Menge von Tupeln, wobei jedes jeweils ein Element aus A_1 in Beziehung setzt mit einem Element aus A_2 und gleichzeitig einem aus A_3 und so weiter. Sind beispielsweise A_1 und A_2 die Mengen aller Strings und A_3 die Menge $\{\text{ja}, \text{nein}\}$, so ist die Tabelle `medikament` gerade eine Relation auf A_1 bis A_3.

10.2 Semantik der Prädikatenlogik

10.2.1 Logische Strukturen

10-8 **Von der aussagenlogischen zur prädikatenlogischen Welt**

In der *Aussagenlogik* geben *Welten* an, welche atomaren Aussagen *wahr oder falsch* sind. Formal ist eine aussagenlogische Welt eine *Belegung von Variablen mit Wahrheitswerten*.
In der *Prädikatenlogik* geben *Welten* an, welche Dinge es gibt und welche Prädikate gültig sind. Formal ist eine prädikatenlogische Welt eine *Belegung von Relationssymbolen mit Relationen und von Variablen mit Objekten*.

Merke

1. Aussagenlogische Welt = Belegung von Variablen mit Wahrheitswerten
2. Prädikatenlogische Welt = Belegung von Variablen mit Objekten + Relationen

10-9 **Definition der logischen Struktur.**

Definition

Sei σ eine Signatur. Eine *logische Struktur* $\mathcal{S}$ *zur Signatur* σ ist ein Tupel bestehend aus:

1. Einer nichtleeren Menge U, genannt *Universum*.
2. Für jedes Relationssymbol R in σ der Stelligkeit n einer Relation $R^{\mathcal{S}} \subseteq \underbrace{U \times \cdots \times U}_{n\text{-mal}}$.

Das Universum kann *endlich* oder auch *unendlich* sein.

10-10 **Eine Datenbank . . .**

Beispiel

```
mysql> select * from medikamente;
+-----------+---------------------+------------+
| produkt   | wirkstoff           | zugelassen |
+-----------+---------------------+------------+
| Aspirin   | Acetylsalicylsaeure | true       |
| Homoeofix | null                | true       |
| Zinkofix  | Zink                | true       |
+-----------+---------------------+------------+

mysql> select * from wirkt_gegen;
+---------------------+---------------+
| wirkstoff           | krankheit     |
+---------------------+---------------+
| Acetylsalicylsaeure | Kopfschmerzen |
| Acetylsalicylsaeure | Entzuendungen |
| Zink                | Zinkmangel    |
+---------------------+---------------+
```

. . . als logische Struktur $\mathcal{D}$. 10-11

- Die *Signatur* ist (M^3, W^2).
- Das *Universum* ist die Menge aller Dingen, über die geredet wird, also die Menge aller Produkte, Wirkstoffe und Boole'schen Werte.
- Die Relation $M^{\mathcal{D}}$ zum Relationssymbol M:

$$\begin{aligned} M^{\mathcal{D}} = \{&(\text{Aspirin}, \text{Acetylsalicylsaeure}, \text{true}),\\ &(\text{Homooefix}, \text{null}, \text{true}),\\ &(\text{Zinkofix}, \text{Zink}, \text{true})\} \end{aligned}$$

- Die Relation $W^{\mathcal{D}}$ zum Relationssymbol W:

$$\begin{aligned} W^{\mathcal{D}} = \{&(\text{Acetylsalicylsaeure}, \text{Kopfschmerzen}),\\ &(\text{Acetylsalicylsaeure}, \text{Entzuendungen}),\\ &(\text{Zink}, \text{Zinkmangel})\} \end{aligned}$$

Bemerkungen zur Notation. 10-12

- Ein Relations*symbol* R ist einfach nur ein Symbol (Zeichen) in der Syntax.
- Eine *Relation* entspricht einer Tabelle in der Datenbank, jedoch kann eine Relation auch unendlich sein.
- Um die Relation vom Symbol R zu unterscheiden und da diese Relation in jeder logischen Struktur anders ist, schreibt man die logische Struktur als hochgestellten Index hinzu: $R^{\mathcal{S}}$.
- Um die *Stelligkeit* eines Relationssymbols *in einer Signatur* anzudeuten, schreibt man diese Stelligkeit in der Signatur ebenfalls als hochgestellten Index hinzu: R^3.
- All diese unterschiedlichen Benutzungen von R muss man sauber auseinanderhalten.

10.2.2 Welten

Definition von Welten für die Prädikatenlogik. 10-13

Definition
Sei σ eine Signatur. Eine *Welt W zur Signatur σ* besteht aus

1. einer logischen Struktur $\mathcal{S}$ zur Signatur σ und
2. einer Variablenbelegung $\alpha\colon X \to U$, wobei $X = \{x, x', x'', \dots\}$ die Menge der Variablen ist und U das Universum von $\mathcal{S}$.

Beispiel zweier Welten zur Signatur $\sigma = (R^2)$. 10-14

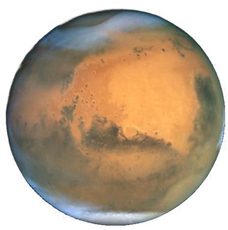
Welt 1

- Universum $U = \{\text{Alice}, \text{Bob}, \text{Charlie}\}$.
- Relation R $= \{(\text{Alice}, \text{Bob}), (\text{Bob}, \text{Charlie})\}$.
- $\alpha(x_1) = \text{Alice}$, $\alpha(x_2) = \text{Bob}$


Authored by NASA, public domain

Welt 2

- Universum $U = \{\text{Binks}, \text{Yoda}, \text{R2D2}\}$.
- Relation R $= \{(\text{Binks}, \text{R2D2})\}$.
- $\alpha(x_1) = \text{Yoda}$, $\alpha(x_2) = \text{Yoda}$


Authored by NASA, public domain

10.2.3 Modellrelation

10-15 **Die Modellrelation in der Prädikatenlogik.**

Zur Erinnerung: In der Aussagenlogik schreiben wir $\beta \models \varphi$, wenn »φ in der Welt β gilt«. Um herauszufinden, ob dies der Fall ist, muss man *die Formel φ unter der Belegung β auswerten*.

Die Dinge liegen nun ganz ähnlich: In der Prädikatenlogik schreiben wir $W \models \varphi$, wenn »φ in der Welt W gilt«. Um herauszufinden, ob dies der Fall ist, muss man *die Formel φ in der Welt W auswerten*.

10-16 **Definition der Modellrelation.**

▶ **Definition**

Sei σ eine Signatur, sei $W = (\mathcal{S}, \alpha)$ eine Welt zur Signatur σ und sei φ eine Formel zur Signatur σ.

Im Folgenden sind nun genau alle Umstände aufgelistet, unter denen $W \models \varphi$ gilt. Wir machen eine Fallunterscheidung nach dem Aufbau von φ:

- φ hat die Form $u = v$ und $\alpha(u) = \alpha(v)$.
- φ hat die Form $R(v_1, \dots, v_n)$ und $\big(\alpha(v_1), \dots, \alpha(v_n)\big) \in R^{\mathcal{S}}$.
- $\varphi = \neg\psi$ und es gilt nicht $W \models \psi$.
- $\varphi = (\psi \wedge \rho)$ und sowohl $W \models \psi$ also auch $W \models \rho$.
- $\varphi = (\psi \vee \rho)$ und $W \models \psi$ oder $W \models \rho$.
- $\varphi = (\psi \to \rho)$ und es gelten nicht sowohl $W \models \psi$ als auch $W \not\models \rho$.
- $\varphi = (\psi \leftrightarrow \rho)$ und es gelten entweder sowohl $W \models \psi$ als auch $W \models \rho$ oder beide gelten gerade nicht.
- $\varphi = \exists v(\psi)$ und es gibt ein Objekt s im Universum U von $\mathcal{S}$, so dass $W' \models \psi$ gilt, wobei $W' = (\mathcal{S}, \alpha')$ und α' unterscheidet sich von α nur dadurch, dass $\alpha'(v) = s$.
- $\varphi = \forall v(\psi)$ und für jedes Objekte $s \in U$ gilt $W' \models \psi$, wobei $W' = (\mathcal{S}, \alpha')$ und sich jedes α' (eines für jedes s) von α nur dadurch unterscheidet, dass $\alpha'(v) = s$.

10-17 ✎ **Zur Übung**

Sei die Signatur $\sigma = (N^2, E^1)$ gegeben. Die logische Struktur $\mathcal{E}$ sei wie folgt aufgebaut:

1. Das Universum enthält die Staaten der Erde.
2. Die Relation $N^{\mathcal{S}}$ ist die Nachbarschaftsrelation. So gilt $(\text{Deutschland}, \text{Polen}) \in N^{\mathcal{S}}$.
3. Die Relation $E^{\mathcal{S}}$ ist die Menge der Staaten der Europäischen Union.

Für die Variablenbelegung α gelte $\alpha(x) = \text{Deutschland}$ und $\alpha(y) = \text{Polen}$. Sei $W = (\mathcal{S}, \alpha)$. Welche der folgenden Modellbeziehungen gelten?

1. $W \models x = y$
2. $W \models N(x,y) \wedge E(x) \wedge E(y)$
3. $W \models \exists z(N(x,z) \wedge \neg E(z))$
4. $W \models \exists x(N(y,x) \wedge \neg E(x))$
5. $W \models \forall z((N(x,z) \wedge N(y,z)) \to \forall w(N(w,z) \to E(w)))$

10.2.4 Semantische Grundbegriffe

10-18 **Der Modellbegriff.**

▶ **Definition**

Eine Welt $W = (\mathcal{S}, \alpha)$ heißt *Modell* einer Formel φ, falls $W \models \varphi$. Eine Welt heißt Modell einer Menge Φ von Formeln, falls sie ein Modell jeder Formel in Φ ist.

Beobachtung

Ist φ geschlossen (hat keine freien Variablen), so hängt es nur von der logischen Struktur $\mathcal{S}$ ab, ob W ein Modell von φ ist. Denn eine Wertzuweisung $\alpha(x) = u$ ist entweder irrelevant, wenn die Variable x in der Formel φ gar nicht vorkommt, oder jedes Vorkommen von x erfolgt nach einem Quantor, so dass die ursprüngliche Belegung von x *überschrieben* wird.

▶ **Definition**

Eine logische Struktur $\mathcal{S}$ heißt *Modell* einer geschlossenen Formel φ, falls $(\mathcal{S}, \alpha) \models \varphi$ für irgendein α (und damit für alle α) gilt.

Tautologien, Erfüllbarkeit und Kontradiktionen sind genauso definiert wie in der Aussagenlogik. 10-19

▶ Definition

Sei σ eine Signatur und φ eine Formel. Dann heißt

1. φ eine *Tautologie*, wenn jede Welt zur Signatur σ ein Modell von φ ist.
2. φ *erfüllbar*, wenn es eine Welt zur Signatur σ gibt, die ein Modell von φ ist.
3. φ eine *Kontradiktion*, wenn φ kein Modell besitzt.

Beispiel

- Die Formel $\forall x(\exists y(x=y))$ ist eine Tautologie.
- Die Formel $\forall x(\forall y(x=y))$ ist erfüllbar, aber keine Tautologie.
- Die Formel $\forall z\big(\exists x\big(\exists y\big((x=z)\wedge(y=z)\wedge\neg(x=y)\big)\big)\big)$ ist eine Kontradiktion.

Zusammenfassung dieses Kapitels

▶ Logische Struktur 10-20

Eine *logische Struktur* $\mathcal{S}$ mit Signatur σ besteht aus einem Universum U und Relationen $R^{\mathcal{S}}$. Dabei gibt es für Relation R in σ genau eine Relation $R^{\mathcal{S}} \subseteq U^n$, wobei n die Stelligkeit von R ist.

▶ Welt

Eine *Welt* $W = (S,a)$ besteht aus einer logischen Struktur S über einem Universums U zusammen mit einer Belegung $a\colon V \to U$ von Variablen mit Objekten des Universums.

▶ Modellrelation

Die *Modellrelation* $\models$ gibt an, ob eine Formel in einer Welt $(\mathcal{S},\alpha)$ gilt:

1. Formeln wie $x=y$ gelten, wenn x und y in der Welt *dasselbe »Ding« beschreiben,* also $\alpha(x)=\alpha(y)$.
2. Formeln wie $R(x,y)$ gelten, wenn x und y in der Welt *»Dinge« beschreiben, die in Relation stehen,* also $(\alpha(x),\alpha(y)) \in R^{\mathcal{S}}$.
3. Junktoren wie $\neg$ und $\wedge$ funtionieren wie in der Aussagenlogik.
4. Die Formeln $\exists x(\psi)$ ist wahr, wenn man *wenigstens ein »Ding«* für x einsetzen kann, so dass ψ wahr wird.
5. Die Formeln $\forall x(\psi)$ ist wahr, wenn man *jedes beliebige »Ding«* für x einsetzen kann, und ψ wird wahr.

▶ Semantische Begriffe

Die *semantischen Begriffe* »Modell«, »Tautologie«, »Erfüllbarkeit« und »Kontradiktion« sind analog definiert wie in der Aussagenlogik.

Übungen zu diesem Kapitel

Übung 10.1 Länder der Erde, mittel

Wir betrachten eine prädikatenlogische Welt $W = (\mathcal{S}, \alpha)$ mit Signatur $\tau = (N^2, E^1, M^1, Z^2)$. Die Struktur

$$\mathcal{S} = (U, N^{\mathcal{S}}, E^{\mathcal{S}}, M^{\mathcal{S}}, Z^{\mathcal{S}})$$

enthält als Universum U die Menge alle Staaten der Erde. Weiterhin definiert die Struktur $\mathcal{S}$ die Relation $N^{\mathcal{S}}$ als die »Grenzt an«-Relation, beispielsweise gelten

$$(\text{Deutschland}, \text{Polen}) \in N^{\mathcal{S}},$$
$$(\text{Deutschland}, \text{Island}) \notin N^{\mathcal{S}}.$$

Die Relation $E^{\mathcal{S}}$ bedeutet »liegt in Europa«, also Luxemburg $\in E^{\mathcal{S}}$, aber China $\notin E^{\mathcal{S}}$. Weiterhin steht $M^{\mathcal{S}}$ für »liegt am Meer«, zum Beispiel Dänemark $\in M^{\mathcal{S}}$, aber Äthiopien $\notin M^{\mathcal{S}}$. Schließlich beschreibt $Z^{\mathcal{S}}$ die Relation »liegen (teilweise) in derselben Zeitzone«, zum Beispiel $(\text{USA}, \text{Peru}) \in Z^{\mathcal{S}}$, $(\text{USA}, \text{Algerien}) \notin Z^{\mathcal{S}}$.

Bei Formeln, die eine ungebundene Variable wie etwa x enthalten, kann man sich nun fragen, für welche Werte von $\alpha(x)$ sie wahr werden. Beispielsweise gilt die Formel $E(x) \wedge \neg\exists y(N(y,x))$ nur, wenn $\alpha(x)$ ein europäischer Staat ist, der an keinen anderen Staat grenzt. Dies gilt nur für $\alpha(x) = \text{Island}$ und für $\alpha(x) = \text{Malta}$. (Beachten Sie, dass Färöer kein souveräner Staat ist und Zypern nicht in Europa liegt.)

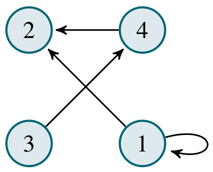
1. Geben Sie eine prädikatenlogische Formel zur Signatur τ an, die nur dann in der Welt W erfüllt ist, wenn $\alpha(x) = \text{Liechtenstein}$ gilt.
2. Welches Land muss $\alpha(x)$ sein, damit die Formel

$$E(x) \wedge \exists y(N(x,y)) \wedge \forall y(N(x,y) \to \neg Z(x,y))$$

in der Welt W gilt?

Übung 10.2 Graphen als logische Strukturen, mittel

Ein *(gerichter) Graph* ist ein Paar (V, A) bestehend aus einer endlichen, nichtleeren Menge V von *Knoten* und einer Relation $A \subseteq V \times V$, deren Elemente *Kanten* heißen. Die folgende Abbildung stellt beispielsweis den Graphen mit $V = \{1,2,3,4\}$ und $A = \{(1,1),(1,2),(3,4),(4,2)\}$ dar.



Eine prädikatenlogische Struktur $\mathcal{S} = (U, E^{\mathcal{S}})$ über der Signatur $\tau = (E^2)$ kann demnach als Graph mit Knotenmenge U und Kantenrelation $E^{\mathcal{S}}$ aufgefasst werden und umgekehrt. Mittels prädikatenlogischer Formeln können also Aussagen über Graphen ausgedrückt werden. So besagt die Formel $\exists x(\exists y(E(x,y)))$, dass eine Kante existiert. Diese Formel wird genau von den Welten erfüllt, deren Struktur einem Graphen entspricht, der eine Kante hat; also beispielsweise von dem oben abgebildeten Graphen. (Beachten Sie, dass hier die Variablenbelegung der Welt irrelevant ist, da die Formel alle Variablen bindet.)

Geben Sie zu folgenden Formeln an, ob sie in den Welten, deren Struktur dem oben abgebildeten Graphen entspricht, gelten.

1. $\forall x(\exists y(E(x,y)))$,
2. $\exists x(\exists y(E(x,y)) \wedge \exists y(E(y,x)))$.

Übung 10.3 Cliqueneigenschaften beschreiben, mittel

Geben Sie eine Formel an, die beschreibt dass ein gerichter Graph (im Sinne von Übung 10.2) eine *Clique* ist (jeder Knoten ist mit jedem anderen durch eine Kante verbunden).

Für Ihre Formel φ soll also gelten, dass $(\mathcal{S}, \alpha) \models \varphi$ genau dann gilt, wenn $\mathcal{S}$ eine Clique ist und α beliebig ist.

Übung 10.4 Kurze Wege beschreiben, leicht

Geben Sie analog zur vorherigen Übung eine Formel an, die beschreibt, dass in dem Graphen gibt es einen Weg der Länge 3 gibt (also eine Folge von vier Knoten t, u, v, w, so dass eine Kante von t nach u, eine von u nach v und eine von v nach w verläuft).

Übung 10.5 Tournaments beschreiben, mittel

Geben Sie analog zu den vorherigen Übung eine Formel an, die beschreibt, dass der Graph ein *Tournament* ist. Das bedeutet, zwischen zwei verschiedenen Knoten gibt es immer genau eine Kante (entweder in die eine oder in die andere Richtung) und es gibt keine Schlaufen (Kanten von einem Knoten zu sich selbst).

Übung 10.6 Färbbarkeit beschreiben, schwer

In dieser Aufgabe betrachten wir in Erweiterung von Übung 10.2 Graphen, deren Knoten mit einer der drei Farben rot, grün oder blau *gefärbt* werden können. Dazu führen wir drei einstellige Prädikatssymbole R, G und B ein und erhalten so eine Signatur $\sigma = (E^2, R^1, G^1, B^1)$. Entsprechend betrachten wir Strukturen $\mathcal{S} = (U, E^{\mathcal{S}}, R^{\mathcal{S}}, G^{\mathcal{S}}, B^{\mathcal{S}})$ über dieser Signatur.

Ein ungerichteter Graph heißt nun *3-gefärbt*, wenn jeder Knoten mit einer der drei Farben gefärbt ist, so dass keine zwei durch eine Kante verbundenen Knoten dieselbe Farbe haben.

Geben Sie eine prädikatenlogische Formel φ an, so dass eine Welt $W = (\mathcal{S}, \alpha)$ genau dann ein Modell für φ ist, wenn der durch $\mathcal{S}$ beschriebene Graph ungerichtet und 3-gefärbt ist. Die Formel sollte aus zwei Teilformeln bestehen, die beschreiben, dass

1. jeder Knoten genau eine Farbe hat und
2. der Graph 3-gefärbt ist.

Übung 10.7 Cliquen beschreiben, mittel

Ein Graph hat eine *4-Clique*, wenn es vier Knoten in ihm gibt, die alle paarweise miteinander durch eine Kante verbunden sind.

Geben Sie eine prädikatenlogische Formel ψ an, so dass eine Welt $W = (\mathcal{S}, \alpha)$ genau dann ein Modell für ψ ist, wenn der durch $\mathcal{S}$ beschriebene Graph eine 4-Clique besitzt.

Übung 10.8 Beweise führen, schwer

Seien φ_1, φ_2 und ψ prädikatenlogische Formeln. Zeigen Sie: $\{\varphi_1, \varphi_2\} \models \psi$ gilt genau dann, wenn $\varphi_1 \wedge \varphi_2 \models \psi$ gilt.

Übung 10.9 Äquivalenzen nachweisen, schwer

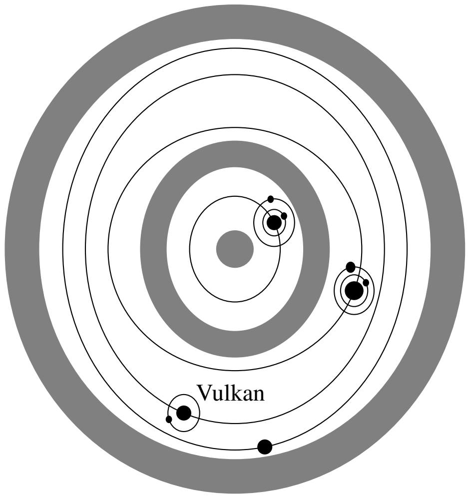
Seien φ und ψ prädikatenlogische Formeln. Zeigen Sie die folgenden Äquivalenzen:

1. $\neg\forall x(\varphi) \equiv \exists x(\neg\varphi)$,
2. $\neg\exists x(\varphi) \equiv \forall x(\neg\varphi)$,
3. $\forall x(\varphi) \to \exists x(\psi) \equiv \exists x(\varphi \to \psi)$.

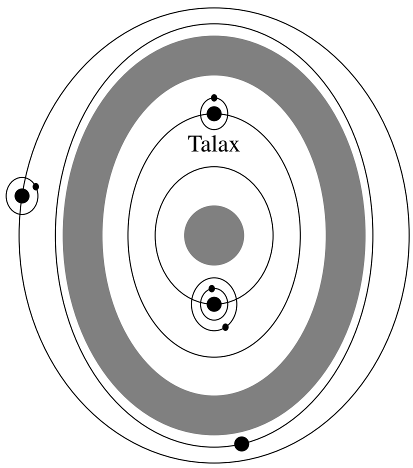
Übung 10.10 Eigenschaften von Sonnensystemen erkennen und beschreiben, mittel

Auf der Voyager unterhalten sich der vulkanische Sicherheitsoffizier Tuvok und der Talaxianer Neelix über die Sonnensysteme ihrer Heimatplaneten. Tuvok formuliert seine Aussagen hierüber natürlich mathematisch präzise mithilfe prädikatenlogischer Formeln und verwendet dabei als Grundlage die Signatur (B^2, M^2, A^1). Auch Neelix schliesst sich dieser Formalisierung an, denn ein Sonnensystem lässt sich nun als Welt $W = (\mathcal{S}, \alpha)$ mit der Struktur $\mathcal{S} = (U, B^{\mathcal{S}}, M^{\mathcal{S}}, A^{\mathcal{S}})$ beschreiben, wobei U alle Planeten und Monde des Systems umfasst, die Relation $B^{\mathcal{S}}$ alle Paare von Planeten enthält, deren Umlaufbahnen direkt benachbart ist, die Relation $M^{\mathcal{S}}$ ein Paar $(a,b) \in U \times U$ enthält, falls b ein Mond von a ist, und $A^{\mathcal{S}}$ alle Planeten umfasst, die an einen Asteroidengürtel grenzen. Der Bordcomputer stellt die beiden Systeme folgendermaßen dar:

Eridani System



Dexa System



Tuvok gibt die folgenden Formeln an woraufhin Neelix überprüft, in welchen Systemen sie gelten. Geben auch Sie für jede Formel und jedes System an, ob das System ein Modell für die Formel ist.

1. $\exists x(\exists y(\exists z(M(z,x) \wedge M(z,y) \wedge A(z) \wedge \neg x = y)))$
2. $\exists x(A(x) \wedge \forall y(B(x,y) \rightarrow \neg \exists z(\neg z = y \wedge B(x,z))))$
3. $\forall x(A(x) \rightarrow \exists x'(\exists x''(\neg x' = x'' \wedge M(x,x') \wedge M(x,x''))))$

Neelix möchte Tuvok nun ebenfalls eine Aufgabe stellen. Helfen Sie ihm mit den folgenden Formeln aus:

4. Eine Formel φ, die genau dann im Dexa System erfüllt ist, falls $\alpha(x) =$ Talax gewählt wird.
5. Eine Formel ψ, die genau dann im Eridani System erfüllt ist, fall $\alpha(x) =$ Vulkan.

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

16 min

Prüfungsfrage 10.11 Grapheigenschaften beschreiben

→ Lösung

Wir fassen eine prädikatenlogische Struktur $\mathcal{S} = (U, E^{\mathcal{S}})$ über der Signatur $\tau = (E^2)$ als gerichteten Graph mit Knotenmenge U und Kantenrelation $E^{\mathcal{S}}$ auf. Drücken Sie nun folgende Eigenschaften als prädikatenlogische Formeln aus, das heißt geben Sie jeweils eine Formel φ an, so dass $(\mathcal{S}, \alpha) \models \varphi$ nur dann gilt, wenn der durch $\mathcal{S}$ dargestellte Graph die jeweilige Eigenschaft erfüllt.

1. Der Graph enthält einen 3-Kreis, das heißt drei Knoten, so dass der erste mit dem zweiten, der zweite mit dem dritten und der dritte mit dem ersten verbunden ist.
2. Der Durchmesser des Graphen ist höchstens drei, das heißt zwischen zwei beliebigen Knoten gibt es immer einen Pfad der Länge drei oder weniger.

16 min

Prüfungsfrage 10.12 Grapheigenschaften verstehen

→ Lösung

Eine prädikatenlogische Struktur $\mathcal{S} = (U, E^{\mathcal{S}})$ über der Signatur $\tau = (E^2)$ kann man als gerichteten Graphen mit Knotenmenge U und Kantenrelation $E^{\mathcal{S}}$ visualisieren. Geben Sie für die folgenden Formeln jeweils ein Modell an mit jeweils *mindestens vier* Elementen (also Knoten) im Universum, indem Sie einen Graphen aufmalen, der als logische Struktur aufgefasst ein Modell der Formel ist.

1. $\forall x \forall y \big(x = y \vee (E(x,y) \wedge E(y,x)\big)$.
2. $\exists x \exists y \exists z \big(E(x,y) \wedge E(y,z) \wedge \neg E(y,z)\big)$.
3. $\exists x \forall y \big(x = y \vee (E(x,y) \wedge \neg E(y,x))\big)$.

8 min

Prüfungsfrage 10.13 Strukturen trennen

→ Lösung

Wir betrachten die Signatur $\tau = (<^2)$. Eine mögliche Struktur zu dieser Signatur ist $\mathcal{Z} = (\mathbb{Z}, <^{\mathcal{Z}})$, das heißt die ganzen Zahlen mit der üblichen »kleiner als«-Relation. Eine weitere Struktur sind die rationalen Zahlen $\mathcal{Q} = (\mathbb{Q}, <^{\mathcal{Q}})$, wobei die Relation ebenfalls auf die übliche Weise definiert ist. Beachten Sie, dass die Konstantensymbole 0 und 1 nicht zur Verfügung stehen.

Geben Sie eine Formel an, die in $\mathcal{Q}$ gilt, aber nicht in $\mathcal{Z}$.

16 min

Prüfungsfrage 10.14 Grapheigenschaften beschreiben

Geben Sie genau wie in Prüfungsfrage 10.11 Formeln für folgende Grapheigenschaften an:

1. Es gibt zwei Knoten im Graphen, die den Abstand höchstens vier haben. Der Abstand zweier Knoten ist die Länge eines kürzesten Weges vom einen zum anderen Knoten, wobei die Länge eines Weges der Anzahl der vorkommenden Kanten entspricht.
2. Es gibt einen Knoten im Graphen mit Exzentrizität drei. Die Exzentrizität eines Knotens ist der Abstand zu einem am weitesten entfernten Knoten im Graphen.
3. Der Radius des Graphen beträgt drei, das heißt die kleinste bei einem Knoten im Graphen vorkommende Exzentrizität ist drei.

15 min

Prüfungsfrage 10.15
Beweise führen

Seien φ, ψ und ρ prädikatenlogische Formeln, wobei in ψ die Variable x nicht vorkommt. Zeigen Sie die folgenden Äquivalenzen:

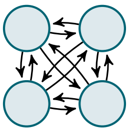
1. $\exists x(\varphi) \vee \psi \equiv \exists x(\varphi \vee \psi)$
2. $\exists x(\varphi) \wedge \forall x(\rho) \equiv \exists x(\varphi \wedge \rho)$

Lösung zu 10.11

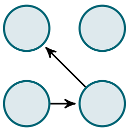
1. $\exists x \exists y \exists z\big(E(x,y) \wedge E(y,z) \wedge E(z,x) \wedge \neg x = y \wedge \neg y = z \wedge \neg x = z\big)$.
2. $\forall x \forall y \exists z \exists w\big(x = y \vee E(x,y) \vee (E(x,z) \wedge E(z,y)) \vee (E(x,z) \wedge E(z,w) \wedge E(w,y))\big)$

Lösung zu 10.12

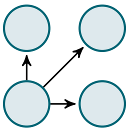
1. Modell der Formel $\forall x \forall y\big(x = y \vee (E(x,y) \wedge E(y,x)\big)$:



2. Modell der Formel $\exists x \exists y \exists z\big(E(x,y) \wedge E(y,z) \wedge \neg E(y,z)\big)$:



3. Modell der Formel$\exists x \forall y\big(x = y \vee (E(x,y) \wedge \neg E(y,x))\big)$:



Lösung zu 10.13

$$\forall x \forall y\big(x < y \rightarrow \exists z(x < z \wedge z < y)\big).$$

Erläuterung: In $\mathbb{Q}$ gibt es »zwischen« je zwei Zahlen eine weitere (man sagt, die rationalen Zahlen sind »dicht«), in $\mathbb{Z}$ hingegen nicht.

Lösung zu 11.1

Eine Signatur, zu der beide Formeln passen, ist

$$\sigma = (g^1, A^1, B^2, R^2).$$

Eine mögliche Struktur $\mathcal{S}$ zur Signatur σ besteht aus

- dem Universum $U^{\mathcal{S}} = \mathbb{N}$ der natürlichen Zahlen,
- der Funktion $g^{\mathcal{S}}(x) = x$,
- den Relationen $A^{\mathcal{S}} = \{x \mid \text{x ist prim}\}$, $B^{\mathcal{S}} = \{(x,y) \mid y = x+1\}$ und $R^{\mathcal{S}} = \{(x,y) \mid y < x\}$.

Lösung zu 11.4

Beide Formeln sind weder tautologisch noch kontradiktorisch.

1. Modell: Die Struktur $\mathcal{A}$ besteht aus dem Universum $U^{\mathcal{A}} = \{0\}$ und den Relationen $T^{\mathcal{A}} = \{0\}$ und $B^{\mathcal{A}} = \emptyset$.
   Kein Modell: Die Struktur $\mathcal{B}$ besteht aus dem Universum $U^{\mathcal{B}} = \{0\}$ und den Relationen $T^{\mathcal{B}} = \emptyset$ und $B^{\mathcal{B}} = \emptyset$.
2. Modell: Die Struktur $\mathcal{C}$ besteht aus dem Universum $U^{\mathcal{C}} = \mathbb{N}$, der Funktion $f^{\mathcal{C}}(x) = x+1$ und $R^{\mathcal{C}} = \{(1,2)\}$.
   Kein Modell: Die Struktur $\mathcal{D}$ besteht aus dem Universum $U^{\mathcal{D}} = \mathbb{N}$, der Funktion $f^{\mathcal{D}}(x) = x+1$ und der Relation $R^{\mathcal{D}} = \{(x,y) \mid y < x\}$.

Lösung zu 11.5

1. Eine Signatur, zu der die Formel passt, ist

$$\sigma = (f^1, g^1, R^2, T^1).$$

2. Ein Modell ist z.B. die logische Struktur $\mathcal{S}$ mit
   - dem Universum $U^{\mathcal{S}} = \{1\}$,
   - den Funktionen $f^{\mathcal{S}}(x) = g^{\mathcal{S}}(x) = x$,
   - den Relationen $R^{\mathcal{S}} = \{(1,1)\} = U^{\mathcal{S}} \times U^{\mathcal{S}}$ sowie weiterhin $T^{\mathcal{S}} = \{1\} = U^{\mathcal{S}}$.
3. Kein Modell ist z.B. die logische Struktur $\mathcal{S}$ mit
   - dem Universum $U^{\mathcal{S}} = \{1\}$,
   - den Funktionen $f^{\mathcal{S}}(x) = g^{\mathcal{S}}(x) = x$,
   - den Relationen $R^{\mathcal{S}} = \emptyset$ und $T^{\mathcal{S}} = \emptyset$.

11-1

Kapitel 11

Terme

Von Tischen, Stühlen und Bierseideln

11-2

Lernziele dieses Kapitels

1. Die Begriffe Konstantensymbol, Funktionssymbol und Term kennen und anwenden können
2. Das Konzept der Substitution kennen und anwenden können

Inhalte dieses Kapitels

Im ersten Kapitel über Beweissysteme wurde Ihnen stolz verkündet, »$1+1=2$« sei eine der unumstößlichen Wahrheiten der Mathematik. Auch in der Populärmusik wird diese Wahrheit als so evident angesehen, dass die Formel in einem Lied von Frau H. Knef als Begründung dafür herhalten muss, dass man doch lieber küssen und nicht denken solle. Worum es heute geht

Die Formel »$1+1=2$« ist allerdings (noch) keine Formel im Sinne der Prädikatenlogik. Weder lassen sich Junktoren noch Quantoren noch überhaupt Variablen entdecken. Man könnte diesen Umstand einfach ignorieren und darauf bestehen, dass die Formel gefälligst irgendwie »umgeschrieben« werden solle mit Hilfe von Relationssymbolen und Variablen und Quantoren. Das wird in der Tat manchmal auch gemacht, ist aber reichlich umständlich und unnatürlich. Viel besser ist es, die Syntax der Prädikatenlogik dahingehend zu erweitern, dass *Terme* wie »$1+1$« fester Bestandteil sowohl der Syntax wie auch der Semantik werden. Genau darum geht es in diesem Kapitel.

Wenn man sein mathematisches Glaubensgebäude vollkommen gefestigt hat und den wahren Glauben gewonnen hat, dass $1+1=2$ eine unumstößlich wahre Formel ist, so ist man doch etwas indigniert, in einem Mathematiklehrbuch über Topologie zu lesen: »…, wobei in obiger Rechnung benutzt wurde, dass natürlich $1+1=0$ gilt…« Wie kommen solch satanische Verse zu Stande? Die Autoren des Buches haben in diesem Absatz im Galois-Körper $GF(2)$ gerechnet – was im Wesentlichen bedeutet, dass sie nicht bis Zwei zählen wollen.

Wie dem auch sei, ist $1+1=2$ oder doch eher $1+1=0$? Stellt man die Frage anders, so ist sie leichter zu beantworten: Gilt $R(c,d)$ oder doch eher $R(c,e)$? Benutzt man ein Relationssymbol wie R und Buchstaben wie c, d und e, so ist klar, dass die Wahrheit einer Formel von der Welt abhängt. Bei der Formel $1+1=2$ hängt es *auch* von der Welt ab, ob dies der Fall ist – es fällt uns nur viel schwerer, dies einzusehen, da wir eine vorgefasste Meinung haben, was die Symbole »1« und »+« bedeuten.

Von Vorurteilen müssen Sie sich in diesem Kapitel lösen; und wo Sie schon dabei sind, sollten Sie auch Ihre gut gepflegten sonstigen Vorurteile betreffend das Leben im Allgemeinen kurz überdenken. Wenn in einer Formel ein Symbol wie »1« vorkommt, so bedeutet dies ersteinmal *gar nichts*. Erst die Welt legt fest, was dieses Symbol konkret bedeutet. Gewissermaßen zufälligerweise kann in einer Welt dieses Symbol auch gerade die natürliche Zahl Eins meinen, das Symbol kann aber sehr gut auch für einen Bierkrug stehen.

Zugegeben, die Trennung in Syntax (Regeln, wie man lustige Symbolfolgen bilden kann) und Semantik (die Lehre davon, was diese lustigen Symbolfolgen so alles bedeuten könnten) wird hier auf die Spitze getrieben. Es wird darauf bestanden, dass die aus drei Symbolen bestehende Zeichenkette $1+1$ zwar syntaktisch korrekt ist, aber genauso viel bedeutet wie ♣♡♣. Gnädig wird dann hinterher diesen Zeichenkette eine Bedeutung gegeben, unter Umständen wird anerkannt, dass die Zeichenkette $1+1$ vielleicht zur Zahl Zwei auswertet, es wird aber darauf bestanden, dass es genauso gut auch die Null sein könnte. Oder eben ein Bierseidel – zum Wohl.

11.1 Syntaktische Erweiterungen

11-4 **Wiederholung: Die Syntax und Semantik der Prädikatenlogik bisher.**

- **Signatur** Gibt an, welche *Relationssymbole* es gibt.
- **Universum** Eine nichtleere Menge, die die Dinge enthält, über die wir reden wollen.
- **Struktur** Gibt an, wie die Relationssymbole *interpretiert werden*. Eine Struktur $\mathcal{S}$ enthält für jedes Relationssymbol R der Stelligkeit n eine n-stellige Relation $R^{\mathcal{S}} \subseteq U^n$.
- **Welt** Sie besteht aus einer logischen Struktur zusammen mit einer Belegung der Variablen mit Objekten (Elementen des Universums).
- **Variablen** Syntaktische Gebilde, die für Dinge stehen.
- **Formeln** Syntaktische Gebilde, die in einer Welt wahr oder falsch sein können.

11-5 **Wodurch wir die Syntax und Semantik nun erweitern.**

Im Folgenden *erweitern* wir die Syntax und die Semantik durch die hervorgehobenen Konzepte.

Syntaktisches Konzept	Semantische Entsprechung
Variable	Element des Universums
Formel	Gültigkeit in einer Welt
Relationssymbol	Relation
Funktionssymbol	Funktion
Konstantensymbol	festes Element des Universums
Term	Auswertung

11.1.1 Funktionssymbole

11-6 **Ein Problem aus der Programmverifikation.**

Bei der *Programmverifikation* versucht man *zu beweisen, dass ein Programm korrekt ist*. Man spezifiziert durch prädikatenlogische Formeln, was *vor* und was *nach* Ausführung des Programms gelten soll.

```
int min (int x, int y) {
  int z = x;

  // Jetzt gilt: z = x
  if (y < x)
    z = y;
  // Jetzt gilt: z ist das Minimum von x und y
}
```

Wir wollen den Text »z ist das Minimum von x und y« als Formel aufschreiben. Mit *Relationssymbolen* ist dies etwas unschön: Man schreibt »$M(x,y,z)$« und verlangt, dass $M^{\mathcal{S}}$ die Relation ist, die alle Tripel enthält, in denen die dritte Komponente das Minimum der ersten beiden ist. Viel *schöner* ist es, wenn wir schreiben können $z = \min(x,y)$.

Erweiterung der Syntax um Funktionssymbole. 11-7

Wir führen folgende *Erweiterungen der Syntax* durch:

1. *Signaturen* können neben Relationssymbolen nun auch *Funktionssymbole* enthalten.
2. Genau wie bei den Relationssymbolen wird durch die Signatur jedem Funktionssymbol auch *eine positive Stelligkeit* zugeordnet.
3. Genau wie bei den Relationssymbolen wird diese Stelligkeit innerhalb der Signatur als *hochgestellter Index* geschrieben.
4. Wir verwenden *Kleinbuchstaben* für Funktionssymbole.

Beispiel

Die Signatur $\tau = (E^2, R^3, f^1, g^2, T^1)$ enthält drei Relationssymbole (E, R und T) und zwei Funktionssymbole (f und g).

Erweiterung der Semantik um Funktionen. 11-8

Wir führen folgende *Erweiterungen der Semantik* durch:

1. *Logische Strukturen* $\mathcal{S}$ können neben Relationen nun auch *Funktionen* enthalten.
2. Für jedes n-stelliges Funktionssymbol f in σ enthält $\mathcal{S}$ eine Funktion $f^{\mathcal{S}}\colon U^n \to U$.
3. Zur Erinnerung: Die Schreibweise $f^{\mathcal{S}}\colon U^n \to U$ bedeutet, dass $f^{\mathcal{S}}$ eine Funktion ist, die jedem Tupel bestehend aus n Elementen des Universums U ein Element des Universums zuordnet.

Beispiel

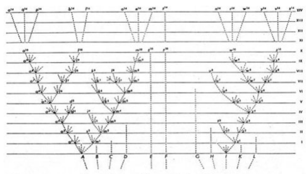
Eine logische Struktur $\mathcal{N}$ zur Signatur $\tau = (f^2)$ könnte das Universum $\mathbb{N}$ haben und $f^{\mathcal{N}}$ könnte die Additionsfunktion sein.

✎ Zur Übung 11-9

Die logische Struktur $\mathcal{B}$ des Baum des Lebens hat als Universum alle Spezies, die es gibt und jemals gab.

Geben Sie für folgende Konzepte jeweils an, ob sie mit Relationssymbolen oder mit Funktionssymbolen beschrieben werden sollten. Geben Sie auch die Stelligkeit an.

1. Die Spezies ist ein Vorfahr einer anderen Spezies.
2. Die Großelternspezies einer Spezies.
3. Der jüngste gemeinsame Vorfahre zweier Spezies.
4. Die Spezies ist nicht ausgestorben.



Tree Diagram from *Origin of Species*

Author Charles Darwin, Public Domain

11.1.2 Konstantensymbole

Noch einmal Programmverifikation. 11-10

Wir wollen eine leicht abgewandelte Version des Programms verifizieren:

```
int min (int x, int y) {
  int z = 0;

  // Jetzt gilt: z ist gleich 0
  if (y < x)
    z = y;
  else
    z = x;
  // Jetzt gilt: z = min(x,y)
}
```

Die Formeln am Ende bereit kein Problem mehr, denn wir können ein *zweistelliges Funktionssymbol* min verwenden. Die erste Formel ist nun das Problem, denn $z = 0$ können wir nicht schreiben, da 0 keine Variable ist.

11-11 **Erweiterung der Syntax um Konstantensymbole.**

Wir führen folgende *Erweiterungen der Syntax* durch:

1. *Signaturen* können neben Relations- und Funktionssymbolen nun auch *Konstantensymbole* enthalten.
2. Konstanten haben *keine Stelligkeit*.
3. Sie werden in einer Signatur durch den *hochgestellten Index 0* angedeutet.
4. Wir verwenden *Kleinbuchstaben* für Konstantensymbole.

Beispiel

Die Signatur $\tau = (E^2, f^2, s^0, t^0)$ enthält ein Relationssymbol (E), ein Funktionssymbol (f) und zwei Konstantensymbole (s und t).

11-12 **Erweiterung der Semantik um Konstanten.**

Wir führen folgende *Erweiterungen der Semantik* durch:

1. *Logische Strukturen* $\mathcal{S}$ können neben Relationen und Funktionen nun auch *Konstanten* enthalten.
2. Für jedes Konstantensymbol c in σ enthält $\mathcal{S}$ eine Konstante $c^{\mathcal{S}} \in U$.

Beispiel

Eine logische Struktur $\mathcal{N}$ zur Signatur $\tau = (s^0, t^0)$ könnte das Universum $\mathbb{N}$ haben und $s^{\mathcal{N}} = 23$ und $t^{\mathcal{N}} = 42$.

11-13 **Besondere Notationen.**

In der Praxis benutzt man neben Kleinbuchstaben auch *besondere Symbole für Konstanten- und Funktionssymbole*. Beispielsweise könnte man das Konstantensymbol 0 verwenden, für das dann $0^{\mathcal{N}}$ sinnigerweise gerade die Zahl 0 ist. Weiter könnte man $+$ als Funktionssymbol verwenden und $+^{\mathcal{N}}$ wäre gerade die Additionsfunktion. Statt $+(x,y)$, was man auch die *Präfix-Schreibweise* nennt, schreibt man dann besser $x+y$, was sich auch *Infix-Schreibweise* nennt.

11-14 **Suggestive Notationen sind gefährlich.**

Extreme Vorsicht ist geboten

Zwar wird oft durch die *Bezeichnung der Funktionssymbole oder Konstantensymbole* eine bestimmte logische Struktur *suggeriert*, es ist aber trotzdem *jede Struktur möglich*.

Beispiel

Die Signatur $\sigma = (0^0, 1^0, +^2)$ enthält zwei Konstantensymbole (0 und 1) und ein zweistelliges Funktionssymbol ($+$). Dann ist eine *völlig legitime* logische Struktur hierzu $\mathcal{M}$, deren Universum $\mathbb{Z}$ ist und in der $0^{\mathcal{M}} = 42$ und $1^{\mathcal{M}} = 23$ und $+^{\mathcal{M}}(a,b) = 6a^2 - 3b$ für alle a und b gilt.

Moral

Suggestive Schreibweisen sind in der Logik eher hinderlich. Hilbert hat deshalb sinngemäß gesagt: »Es muss egal sein, ob man von Punkten, Gerade und Ebene spricht oder von Tischen, Stühlen und Bierseideln.«

11.1.3 Terme und Auswertung

11-15 **Funktions- und Konstantensymbole in Formeln.**

Um Funktions- und Konstantensymbole in Formeln zu benutzen, brauchen wir *Terme*.

▶ Definition

Sei σ eine Signatur. Ein *Term* zu dieser Signatur ist ein Wort t einer der folgenden Bauarten:

1. t ist eine der Variablen x, x', x'', …
2. t ist ein Konstantensymbol aus σ.
3. t hat die Form $f(t_1, \dots, t_n)$, wobei f ein Funktionssymbol aus σ der Stelligkeit n ist und jedes t_i ein Term ist.

Beispiel
Sei $\sigma = (s^0, t^0, f^2, g^1)$. Dann sind folgende Wörter Terme:

- t
- $f(x, g(g(t)))$
- $f(s, f(t, x'))$

Neue Definition von atomaren Formeln. 11-16

Zur Erinnerung: *Atomare Formeln* waren definiert als Wörter der folgenden Formen:

1. $v_1 = v_2$, wobei v_1 und v_2 Variablen sind.
2. $R(v_1, \dots, v_n)$, wobei R ein Relationssymbol der Stelligkeit n ist und die v_i Variablen sind.

Wir definieren *atomare Formeln* nun *allgemeiner*:

▶ Definition
Eine *atomare Formel* ist ein Wort von einer der folgenden Formen:

1. $t_1 = t_2$, wobei t_1 und t_2 Terme sind.
2. $R(t_1, \dots, t_n)$, wobei R ein Relationssymbol der Stelligkeit n ist und die t_i Terme.

Ausdehnung der Semantik auf die neuen Formeln. 11-17

▶ Definition: Auswertung von Termen
Sei $W = (\mathcal{S}, \alpha)$ eine Welt und t ein Term. Die *Auswertung* $\mathrm{eval}_W(t)$ des Terms t ist wie folgt definiert:

Bauart von t	Auswertung $\mathrm{eval}_W(t)$
v	$\alpha(v)$
c	$c^{\mathcal{S}}$
$f(t_1, \dots, t_n)$	$f^{\mathcal{S}}\big(\mathrm{eval}_W(t_1), \dots, \mathrm{eval}_W(t_n)\big)$

▶ Definition: Gültigkeit atomarer Formeln
Für die Gültigkeit von atomaren Formeln definieren wir:

1. $W \models t_1 = t_2$, wenn die Auswertungen von t_1 und t_2 in W gleich sind.
2. $W \models R(t_1, \dots, t_n)$, wenn $\big(\mathrm{eval}_W(t_1), \dots, \mathrm{eval}_W(t_n)\big) \in R^{\mathcal{S}}$.

Beispiel einer Welt und gültiger Formeln. 11-18

Beispiel: Der Baum des Lebens
Sei $\sigma = (N^2, s^0, t^0, f^2)$. Wir definieren eine Welt $W = (\mathcal{B}, \alpha)$ wiefolgt:

- Das Universum U sind alle Spezies (auch ausgestorbene).
- $N^{\mathcal{B}}$ ist die Abstammungsrelation.
- $s^{\mathcal{B}} = \text{Mensch}$
- $t^{\mathcal{B}} = \text{Pferd}$
- $f^{\mathcal{B}}$ bildet ein Paar von Spezies auf den letzten gemeinsamen Vorfahren ab (last common ancestor).
- $\alpha(x) = \text{Huhn}$ und $\alpha(x') = \text{Aal}$.

Es gilt nun:

- $W \models \neg s = t$
- $W \models \exists x(N(s, x) \wedge N(t, x))$
- $W \models \forall x(\forall y(f(x, y) = f(y, x)))$.
- $W \models \neg\exists x(f(x, x') = s)$.

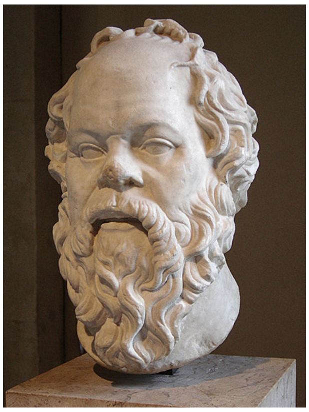
✎ Zur Übung 11-19
Sei $\sigma = (n^0, e^0, p^2)$. Die logische Struktur $\mathcal{N}$ habe das Universum $\mathbb{N}$, es sei $n^{\mathcal{N}} = 0$, $e^{\mathcal{N}} = 1$ und $p^{\mathcal{N}}(a, b) = a + b$. Die logische Struktur $\mathcal{N}'$ sei genauso definiert, nur $p^{\mathcal{N}'}(a, b) = a \cdot b$.
Die Variablenbelegung α sei beliebig.
Welche der folgenden Formeln gelten in der Welt $(\mathcal{N}, \alpha)$ und welche in $(\mathcal{N}', \alpha)$?

1. $p(e, n) = e$
2. $\exists x(p(n, x) = e)$
3. $\forall x(\exists y(\exists z(p(y, z) = x)))$
4. $\forall x(\forall y(p(x, y) = p(n, p(y, x))))$

11.2 Substitution

11.2.1 Idee

11-20 **Eine einfache Erkenntnis.**



- In einer Welt W gelte »alle Menschen werden geboren und müssen sterben«, beziehungsweise
$$W \models \forall x(G(x) \wedge S(x))$$
- Steht das Konstantensymbol s in der Welt für den Menschen Sokrates (also $s^{\mathcal{S}} =$ Sokrates), so gilt in der Welt auch
$$W \models G(s) \wedge S(s)$$
- Steht das Funktionsymbol m für die »Mutterfunktion«, so gilt auch
$$W \models G(m(s)) \wedge S(m(s))$$
- Steht das Funktionsymbol v für die »Vaterfunktion«, so gilt auch
$$W \models G(v(m(s))) \wedge S(v(m(s)))$$

11-21 **Substitution bedeutet »Ersetzen«.**

Unter einer Substitution versteht man allgemein die Ersetzung von etwas durch etwas anderes. In der Logik bedeutet dies etwas konkreter, dass man *eine bestimmte Variable* überall durch einen *bestimmten Term* ersetzt. Genauer: Sei φ eine Formel, v eine Variable und t ein Term. Die *Substitution* von v durch t in φ erhält man, indem an allen Stellen eines *freien Vorkommens* von v in φ statt v nun t geschrieben wird. Wir schreiben $\varphi[v \hookrightarrow t]$ für die durch *die Substitution entstandene Formel*. Alternative Schreibweise für eine Ersetzung sind $\varphi[v \to t]$, $\varphi[v/t]$, $\varphi\frac{v}{t}$, und weitere.

11.2.2 Definition

11-22 **Definition der Substitution**

▶ **Definition**

Seien φ eine Formel, v eine Variable und t ein Term.
Zunächst definiert man die Substitution für Terme τ:

Art des Terms τ	Substitution $\tau[v \hookrightarrow t]$
Variable v	t
Variable u (ungleich v)	u
Konstantensymbol c	c
Funktionsanwendung $f(t_1,\dots,t_n)$	$f(t_1[v \hookrightarrow t],\dots,t_n[v \hookrightarrow t])$

Nun definieren wir die Substitution für Formeln φ:

Art der Formel φ	Substitution $\varphi[v \hookrightarrow t]$
$t_1 = t_2$	$t_1[v \hookrightarrow t] = t_2[v \hookrightarrow t]$
$R(t_1,\dots,t_2)$	$R(t_1[v \hookrightarrow t],\dots,t_n[v \hookrightarrow t])$
$\neg\varphi$	$\neg\varphi[t \hookrightarrow v]$
$(\varphi \circ \psi)$ für Junktoren $\circ$	$(\varphi[v \hookrightarrow t] \circ \psi[v \hookrightarrow t])$
$\forall v(\varphi)$	$\forall v(\varphi)$
$\exists v(\varphi)$	$\exists v(\varphi)$
$\forall u(\varphi)$ für u ungleich v	$\forall u(\varphi[v \hookrightarrow t])$
$\exists u(\varphi)$ für u ungleich v	$\exists u(\varphi[v \hookrightarrow t])$

11-23 ✎ **Zur Übung**

Sei φ die Formel $x = y \wedge \exists x(f(x) = y)$. Wie lauten dann $\varphi[x \hookrightarrow g(y)]$ und $\varphi[y \hookrightarrow h(x, f(y))]$?

Zusammenfassung dieses Kapitels

▶ Konstanten- und Funktionssymbole 11-24

Eine Signatur kann neben Relationssymbolen (Großbuchstaben) auch

- *Konstantensymbole* (Kleinbuchstaben, hochgestellter Index 0) und
- *Funktionssymbole* (Kleinbuchstaben, hochgestellter Index größer 0)

enthalten.

▶ Syntax von Konstanten- und Funktionssymbole: Terme

Terme haben eine der folgende Formen:

1. Eine Variable wie x oder x'.
2. Ein Konstantensymbol wie c oder 0.
3. Ein Funktionssymbol, gefolgt von Termen in Klammern, wie $f(g(x), s(0))$.

▶ Semantik von Konstanten- und Funktionssymbolen

Logische Strukturen $\mathcal{S}$ enthalten für jedes Konstantensymbol c eine *Konstante* $c^{\mathcal{S}}$ und für jedes Funktionssymbolen f eine *Funktion* $f^{\mathcal{S}}$.

Die *Auswertung* eines Terms erhält man, indem man *»die Funktionen so lange anwendet, bis es nicht mehr geht.«*

▶ Substitution

Die *Substitution* einer Variabel v durch einen Term t in einer Formel φ, geschrieben $\varphi[v \hookrightarrow t]$, erhält man, indem man jedes *freie* Vorkommen von v in φ durch t ersetzt.

Übungen zu diesem Kapitel

Übung 11.1 Signatur und Struktur angeben, leicht

Gegeben seien die folgenden zwei prädikatenlogischen Formeln:

$$\forall x(\exists y(g(y) = x) \to R(x,y))$$
$$\exists y(\forall x(R(x,y) \leftrightarrow (A(x) \wedge B(y,y))))$$

1. Geben Sie eine Signatur σ an, zu der beide Formeln gleichzeitig passen.
2. Geben Sie eine logische Struktur zu σ an. (Hinweis: Dabei müssen Sie die beiden Formeln nicht beachten, diese sind unwichtig.)

Übung 11.2 Semantische Eigenschaften überprüfen, schwer

Welche der folgenden Formeln sind erfüllbar, welche Tautologien und welche Kontradiktionen? Es sind P und R Relationssymbole, f und g Funktionssymbole und 0 ein Konstantensymbol.

1. $\forall x(P(x, f(x))) \to \exists y(P(y,y))$,
2. $\exists x(f(x) = x) \wedge \forall x(\neg x = 0 \to \neg x = f(f(x)))$,
3. $(\forall x(f(g(x)) = x) \wedge f(g(0)) = 0) \to g(f(0)) = 0$,
4. $\forall x(\forall y(\neg x = f(x) \wedge (P(x,y) \leftrightarrow x = y))) \to \neg\exists x(P(x, f(x)))$.

Übung 11.3 Semantische Eigenschaften überprüfen, schwer

Wir betrachten die Signatur $\tau = (\leq^2, 0^0, 1^0)$. Eine mögliche Struktur zu dieser Signatur ist $\mathcal{N} = (\mathbb{N}, \leq^{\mathcal{N}}, 0^{\mathcal{N}}, 1^{\mathcal{N}})$, also die natürlichen Zahlen mit der üblichen »kleiner oder gleich«-Relation und den Konstanten Null und Eins. Zwei weitere Strukturen sind die ganzen Zahlen $\mathcal{Z} = (\mathbb{Z}, \leq^{\mathcal{Z}}, 0^{\mathcal{Z}}, 1^{\mathcal{Z}})$ und die rationalen Zahlen $\mathcal{Q} = (\mathbb{Q}, \leq^{\mathcal{Q}}, 0^{\mathcal{Q}}, 1^{\mathcal{Q}})$, wobei die Relationen und Konstanten ebenfalls auf die übliche Weise definiert sind.

Geben Sie eine Formel an, die in $\mathcal{N}$ gilt, aber nicht in $\mathcal{Z}$, eine Formel, die in $\mathcal{Z}$ gilt, aber nicht in $\mathcal{Q}$ und eine Formel, die in $\mathcal{Q}$ gilt, aber nicht in $\mathcal{N}$.

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

Prüfungsfrage 11.4 (15 min) → Lösung

Semantische Eigenschaften von prädikatenlogischen Formeln

Bestimmen Sie für jede der folgenden prädikatenlogischen Formeln, ob sie eine Tautologie ist oder eine Kontradiktion ist oder keines von beiden. Geben Sie für jede Formel, die weder eine Tautologie noch eine Kontradiktion ist, eine Welt an, in der die Formel erfüllt ist, und eine, in der die Formel nicht erfüllt ist. Da die Formeln geschlossen sind (keine freien Variablen haben), müssen Sie keine Variablenbelegung angeben.

1. $\forall x(T(x) \vee \exists y(B(y,x)))$
2. $\exists x(R(x, f(x)))$

Prüfungsfrage 11.5 (12 min) → Lösung

Syntaktische und semantische Eigenschaften untersuchen

Gegeben sei die folgende prädikatenlogische Formel:

$$\forall x(f(x) = 1) \to \exists y(R(g(y), y) \vee T(y))$$

1. Geben Sie eine Signatur σ an, die zu der Formel passt.
2. Geben Sie eine Welt zu σ an, die ein Modell der Formel ist.
3. Geben Sie eine Welt zu σ an, die kein Modell der Formel ist.

Hinweis: Da die Formel geschlossen ist (keine freien Variablen hat), müssen Sie bei den Welten keine Variablenbelegungen angeben.

Prüfungsfrage 11.6 (8 min) → Lösung

Primzahlen beschreiben

Wir betrachten die Signatur $\tau = (m^2, n^0, e^0)$. Eine mögliche Struktur zu dieser Signatur ist $\mathcal{N} = (\mathbb{N}, m^{\mathcal{N}}, n^{\mathcal{N}}, e^{\mathcal{N}})$ mit $m^{\mathcal{N}}(x,y) = x \cdot y$ und $n^{\mathcal{N}} = 0$ und $e^{\mathcal{N}} = 1$. Das heißt, das Funktionssymbol m wird als Multiplikation interpretiert und die Konstantensymbole n und e gerade als Null und Eins.

Geben Sie eine Formel φ an, in der eine freie Variable x vorkommt und für die genau dann $(\mathcal{N}, \alpha) \models \varphi$ gilt, wenn $\alpha(x)$ eine Primzahl ist (also eine Zahl in der Reihe $2, 3, 5, 7, 9, 11, 13, \ldots$).

Prüfungsfrage 11.7 (6 min)

Formeln untersuchen

Welche der folgenden Formeln sind erfüllbar, welche Tautologien und welche Kontradiktionen? Es sind f, g, h Funktionssymbole und P ein Relationssymbol.

1. $\forall x(\neg P(x,0) \wedge f(x) = 0) \to \exists y(\neg P(y, f(y)))$
2. $\forall x(f(g(x)) = x) \to \forall x(g(f(x)) = x)$
3. $\forall x(h(x) = f(g(x))) \wedge \forall y(\exists x(h(x) = y))$
4. $\neg\forall x(f(x) = x) \vee \neg\exists y(f(g(y)) = g(y))$

Prüfungsfrage 11.8 (10 min)

Alternative Quantoren

Wir erweitern die Syntax der bekannten Prädikatenlogik um einen weiteren Quantor, nämlich $\exists!$, mit der Bedeutung »es existiert genau ein«. Syntaktisch funktioniert dieser Quantor wie der gewöhnliche Existenzquantor $\exists$. Allerdings schränken wir die Verwendung von $\exists!$ ein: Die Formel $\exists! x(\varphi)$ ist nur erlaubt, wenn in φ nirgends der Quantor $\exists!$ vorkommt. Erlaubte Formeln sind also $\exists! x(Q(x) \vee P(f(x,y)))$ und $\forall x(Q(x)) \to \exists! x(x = f(x))$.

Die Modellrelation wird wie folgt erweitert. Sei $W = (\mathcal{S}, \alpha)$ eine Welt und φ eine Formel, die $\exists!$ enthalten darf. Zusätzlich zu den üblichen Definitionen ist W nun auch dann ein Modell für φ (das heißt $W \models \varphi$), wenn gilt:

- $\varphi = \exists! v(\psi)$ und es gibt *genau ein* Objekt s im Universum U von $\mathcal{S}$, so dass $W' \models \psi$ gilt, wobei $W' = (\mathcal{S}, \alpha')$ und α' unterscheidet sich von α nur dadurch, dass $\alpha'(v) = s$.

Beschreiben Sie, wie man eine beliebige Formel, die den Quantor $\exists!$ enthält, in eine äquivalente prädikatenlogische Formel ohne diesen Quantor umformen kann.

12 min

Prüfungsfrage 11.9

→ Lösung

Grapheigenschaften beschreiben

Ein Graph hat ein *Königspaar* genau dann, wenn es ein Paar von zwei unterschiedlichen Knoten in dem Graphen gibt, so dass man jeden Knoten in dem Graphen von wenigstens einem der beiden in höchstens zwei Schritten erreichen kann.

Wie gewohnt fassen wir einen Graph mit Knotenmenge V und Kantenrelation $E^{\mathcal{G}} \subseteq V \times V$ als eine prädikatenlogische Struktur $\mathcal{G} = (V, E^{\mathcal{G}})$ über der Signatur $\tau = (E^2)$ auf.

Drücken Sie die Eigenschaft »Der Graph hat ein Königspaar« als prädikatenlogische Formeln aus, das heißt, geben Sie eine Formel φ an, so dass $\mathcal{G} \models \varphi$ genau dann gilt, wenn der durch $\mathcal{G}$ dargestellte Graph ein Königspaar hat.

12 min

Prüfungsfrage 11.10

→ Lösung

Beweis in der Prädikatenlogik führen

Seien φ und ψ prädikatenlogische Formeln. Zeigen Sie, dass gilt

$$(\varphi \wedge \psi) \vee \psi \;\equiv\; \psi.$$

Hinweis: Beachten Sie, dass es sich hier um prädikatenlogische Formeln handelt!

12 min

Prüfungsfrage 11.11

→ Lösung

Grapheigenschaften beschreiben

Ein ungerichteter Graph hat eine k-*Knotenüberdeckung* genau dann, wenn es eine Menge M von höchstens k Knoten gibt, so dass für jede Kante wenigstens einer ihrer beiden Endknoten in M ist.

Wie gewohnt fassen wir einen ungerichteten Graph mit Knotenmenge V und Kantenrelation $E^{\mathcal{G}} \subseteq V \times V$ als eine prädikatenlogische Struktur $\mathcal{G} = (V, E^{\mathcal{G}})$ über der Signatur $\tau = (E^2)$ auf.

Drücken Sie die Eigenschaft »Der Graph hat eine 3-Knotenüberdeckung« als prädikatenlogische Formel aus, das heißt, geben Sie eine Formel φ an, so dass $\mathcal{G} \models \varphi$ genau dann gilt, wenn der durch $\mathcal{G}$ dargestellte Graph eine 3-Knotenüberdeckung besitzt.

10 min

Prüfungsfrage 11.12

→ Lösung

Beweis in der Prädikatenlogik führen

Seien φ und ψ prädikatenlogische Formeln. Zeigen Sie, dass gilt

$$\exists x(\varphi \wedge \psi) \;\models\; \exists x(\varphi) \wedge \exists x(\psi).$$

Lösung zu 11.6

$$\neg\exists a \exists b(m(a,b) = x \wedge \neg a = n \wedge \neg a = e \wedge \neg b = n \wedge \neg b = e).$$

Erläuterung: Eine Zahl x ist *keine* Primzahl, wenn es zwei Zahlen $a, b \geq 2$ gibt mit $a \cdot b = x$. Für natürliche Zahlen a gilt $a \geq 2$ genau dann, wenn $a \neq 1$ und $a \neq 0$.

Lösung zu 11.9

$$\begin{aligned}\varphi = \exists a(\exists b(\neg(a = b) \wedge \forall y(y = a \vee y = b \vee \\ E(a,y) \vee E(b,y) \vee \exists x((E(a,x) \vee E(b,x)) \wedge E(x,y)))))\end{aligned}$$

Erläuterung: Diese Formel ist nur erfüllt, wenn es zwei ungleiche Knoten a und b gibt, so dass jeder Knoten y von a oder b in null Schritten ($y = b$ oder $y = a$), in einem Schritt (es gilt $E(a,y)$ oder $E(b,y)$) oder in zwei Schritten über einen Zwischenknoten x erreicht werden kann.

Lösung zu 11.10

Wir zeigen zwei Richtungen. Zuerst zeigen wir, dass $(\varphi \wedge \psi) \vee \psi \models \psi$. Anschließend werden wir beweisen, dass $\psi \models (\varphi \wedge \psi) \vee \psi$. Laut Definition der Äquivalenz folgt aus den Beweisen der beiden Richtungen dann die Behauptung.

Nun zeigen wir die erste Richtung $(\varphi \wedge \psi) \vee \psi \models \psi$, also dass jedes Modell für $(\varphi \wedge \psi) \vee \psi$ auch ein Modell für ψ ist. Sei M ein beliebiges Modell für $(\varphi \wedge \psi) \vee \psi$. Das heisst, M ist ein Modell für $(\varphi \wedge \psi)$ oder ψ. Wir machen eine Fallunterscheidung und zeigen, dass in jedem Fall M auch ein Modell für ψ ist.

1. M ist ein Modell für $(\varphi \wedge \psi)$. Folglich muss M sowohl ein Modell für φ als auch für ψ sein.
2. M ist ein Modell für ψ.

Für die zweite Richtung $\psi \models (\varphi \wedge \psi) \vee \psi$ zeigen wir, dass jedes Modell für ψ auch ein Modell für $(\varphi \wedge \psi) \vee \psi$ ist. Sei M ein Modell für ψ. Für jede prädikatenlogische Formel ρ gilt dann, dass M auch ein Modell für $\rho \vee \psi$ ist. Sei nun $\rho = (\varphi \wedge \psi)$. Daraus folgt, dass M ein Modell für $(\varphi \wedge \psi) \vee \psi$ ist.

Wir haben beide Richtungen gezeigt, daraus folgt die Behauptung.

Lösung zu 11.11

$$\begin{aligned}\varphi = \exists a(\exists b(\exists c(\forall u(\forall v(E(u,v) \to \\ (a = u \vee b = u \vee c = u \vee a = v \vee b = v \vee c = v))))))\end{aligned}$$

Lösung zu 11.12

Wir wollen zeigen, dass $\exists x(\varphi \wedge \psi) \models \exists x(\varphi) \wedge \exists x(\psi)$ gilt. Dazu müssen wir beweisen, dass jedes Modell für $\exists x(\varphi \wedge \psi)$ auch ein Modell für $\exists x(\varphi) \wedge \exists x(\psi)$ ist.

Sei $(\mathcal{S}, \alpha)$ ein Modell für die Formel $\exists x(\varphi \wedge \psi)$. Dann es gibt ein Element x_0 aus dem Universum von $\mathcal{S}$, so dass für $(\mathcal{S}, \alpha')$ gilt $(\mathcal{S}, \alpha') \models (\varphi \wedge \psi)$, wobei α' identisch ist zu α, außer dass $\alpha'(x) = x_0$ gilt. Dann gilt aber auch $(\mathcal{S}, \alpha') \models \varphi$ und damit auch $(\mathcal{S}, \alpha') \models \psi$. Ersteres impliziert nun aber $(\mathcal{S}, \alpha) \models \exists x(\varphi)$, letzteres $(\mathcal{S}, \alpha) \models \exists x(\psi)$. Also gilt auch $(\mathcal{S}, \alpha) \models \exists x(\varphi) \wedge \exists x(\psi)$.

12-1

Kapitel 12
Hilbertkalkül der Prädikatenlogik
Computer können alles beweisen

12-2

Lernziele dieses Kapitels

1. Axiomensystem für die Prädikatenlogik kennen
2. Aussage des Gödel'schen Vollständigkeitssatzes verstehen
3. Bedeutung des Satzes für die Mathematik und die Informatik einschätzen können

Inhalte dieses Kapitels

Worum es heute geht

Gibt es ein Beweissystem für die Prädikatenlogik? Nun, angesichts des Titels dieses Kapitels liegt es nahe, dass es ein solches gibt, aber klar ist dies keineswegs. Die Prädikatenlogik ist einfach komplizierter als die Aussagenlogik und dies spiegelt sich auch in der Antwort auf die Frage wider, ob es ein Beweissystem gibt.

Bei der Aussagenlogik war von Anfang an klar, *dass* es ein Beweissystem gibt, nämlich die Wahrheitstafeln, vortrefflich streiten ließ sich lediglich um die Frage, ob denn nun die Resolution oder doch eher Hilbertbeweise geeigneter seien. Bei der Prädikatenlogik versagt die Wahrheitstafelmethode kläglich: die Entsprechung dieser Methode in der Prädikatenlogik ist, für eine Formel alle möglichen Welten durchzugehen und zu testen, ob die Formel für alle diese Welten wahr wird. Leider gibt es selbst für völlig banale Formeln wie $x = x$ unendliche viele mögliche Welten, die getestet werden wollen. Zum Vergleich: bei der Aussagenlogik ist die Anzahl der Welten, die bei einer Formel mit n Variablen getestet werden müssen, »nur« 2^n.

Ob eine prädikatenlogische Formel eine Tautologie ist oder nicht, ist ein *semantische* Fragestellung, die wir aber nicht allein durch die Untersuchung von semantischen Begriffen wie Welten und Modellen beantworten können. Es gibt einfach zu viele Welten.

Der Trick besteht darin, die Fronten zu wechseln und zum syntaktischen Lager überzulaufen. Das Beweissystem von Hilbert ist das Flagschiff der syntaktischen Fraktion: Sie erinnern sich vielleicht noch daran, dass in diesem System formalistisch einfach nur Formeln zeilenweise untereinander geschrieben wurden und nur eine einzige Regel, der Modus ponens, beachtet werden muss. Während eines solchen Hilbertbeweises ging *sehr* schnell jegliche Anschauung verloren, was die Formeln *bedeuten*; man war einfach nur glücklich und ermattet, wenn endlich am Ende die gewünschte Formel stand.

In diesem Kapitel werden Sie sehen, dass wir den Hilbertkalkül für Aussagenlogik zu einem für die Prädikatenlogik ausbauen können, einfach indem wir einige neue Axiome hinzufügen. Wie immer sind die Axiome Trivialitäten wie $x = x$. Es war eine der wirklich großen Sternstunden der Mathematik, als Kurt Gödel 1929 bewiesen hat, dass man nur mittels des Modus ponens aus einem solchen Satz von Axiomen *alle prädikatenlogischen Tautologien* herleiten kann.

12.1 Mächtigkeit der Prädikatenlogik

Worum geht es heute? 12-4

Zentrale Fragestellung

Gegeben ist eine prädikatenlogisch Formel φ. *Ist φ eine Tautologie?*

Diese Frage war schon in der Aussagenlogik *nicht ganz einfach zu beantworten*. In der Prädikatenlogik ist sie *noch wesentlich schwieriger* zu beantworten. Im Folgenden werden einige Beispiele vorgestellt, die zeigen, wie schwierig dies sein kann. Es ist deshalb *eher erstaunlich*, dass es trotzdem ein *korrektes und vollständiges Beweisverfahren* für die Prädikatenlogik gibt.

12.1.1 Beispiel: Existenz von Königen

Eine mögliche Tautologie. 12-5

Ist folgende Formel φ_1 eine Tautologie?

$\forall x \forall y \big(E(x,y) \lor E(y,x)\big) \to \exists x \forall y \big(x = y \lor E(x,y) \lor \exists z (E(x,z) \land E(z,y))\big)$

Im Folgenden:

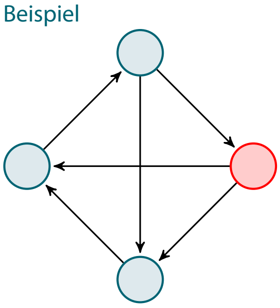
1. Es werden graphtheoretische Deutungen der Formelteile gegeben.
2. Es wird der Satz vom Löwenkönig vorgestellt, der besagt, dass die Formel in jeder endlichen Struktur gilt.
3. Es wird gezeigt, dass die Formel aber trotzdem keine Tautologie ist.

Zwei graphtheoretische Begriffe. 12-6

▶ Definition

- Ein Graph heißt *halbvollständig*, wenn zwischen je zwei Knoten mindestens eine gerichtete Kante verläuft.
- Ein Knoten v eines Graphen heißt ein *König*, wenn alle anderen Knoten von v aus in zwei Schritten erreichbar sind.

Beispiel



Graphtheoretische Deutung der Formelteile. 12-7

Wir benutzen die Signatur $\sigma = (E^2)$ der Graphen. Logische Strukturen hierzu bestehen aus einem Universum (den Knoten) und einer zweistelligen Relation (den Kanten).

Die Formel $\forall x \forall y \big(E(x,y) \lor E(y,x)\big)$

Diese Formel gilt, falls der (durch die Struktur repräsentierte) Graph halbvollständig ist.

Die Formel $\exists x \forall y \big(x = y \lor E(x,y) \lor \exists z (E(x,z) \land E(z,y))\big)$

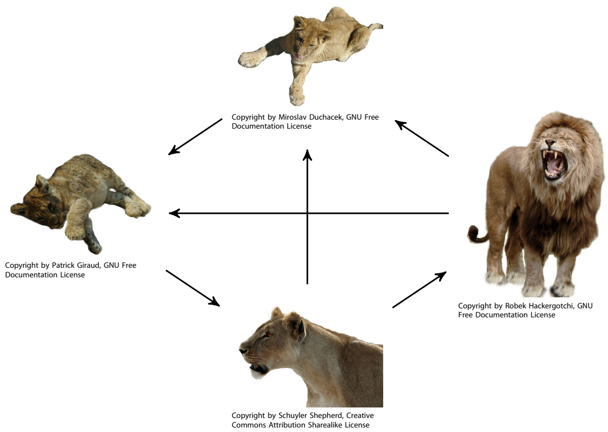
Diese Formel gilt, falls der (durch die Struktur repräsentierte) Graph einen König hat.

Wann ist die Hauptformel eine Tautologie?

Die Formel φ_1 ist genau dann eine Tautologie, wenn $\forall x \forall y \big(E(x,y) \lor E(y,x)\big) \models \exists x \forall y \big(x = y \lor E(x,y) \lor \exists z (E(x,z) \land E(z,y))\big)$, wenn also jeder halbvollständige Graph einen König hat.

12-8 **Das Satz vom Löwenkönig.**

▶ **Satz**
Jeder endliche halbvollständige Graph hat einen König.



12-9 **Die Formel ist trotzdem keine Tautologie.**

Beobachtung
Es gibt *unendliche halbvollständige Graphen*, die keinen König haben.

✎ **Zur Übung:** etwas schwieriger
Geben Sie einen solchen Graphen an.

Folgerung
Die Formel φ_1 ist keine Tautologie.

Merke: *Eine Formel kann in jeder endlichen Welt gelten und trotzdem keine Tautologie sein.*

12.1.2 Beispiel: Körper

12-10 **Ein Tautologie, die einen mathematischen Satz formalisiert.**

▶ **Satz**
$\forall x \forall y \forall z\big((x+y)+z=x+(y+z) \wedge x+y=y+x \wedge 0+x=x \wedge \exists w(w+x=0) \wedge (x \cdot y) \cdot z=x \cdot (y \cdot z) \wedge x \cdot y=y \cdot x \wedge 1 \cdot x=x \wedge \exists w(w \cdot x=1 \vee x=0) \wedge (x+y) \cdot z=(x \cdot z)+(y \cdot z)\big) \to \big(x \cdot y=0 \to (x=0 \vee y=0)\big)$ *zur Signatur* $\sigma=(+^2, \cdot^2, 0^0, 1^0)$ *ist eine Tautologie.*

Beweis. Der erste Formelteil, nämlich die Formel $\forall x \forall y \forall z\big((x+y)+z=x+(y+z) \wedge x+y=y+x \wedge 0+x=x \wedge \exists w(w+x=0) \wedge (x \cdot y) \cdot z=x \cdot (y \cdot z) \wedge x \cdot y=y \cdot x \wedge 1 \cdot x=x \wedge \exists w(w \cdot x=1 \vee x=0) \wedge (x+y) \cdot z=(x \cdot z)+(y \cdot z)\big)$ gilt genau dann in einer logischen Struktur, wenn diese ein *Körper* ist. Die Formel $x \cdot y=0 \to (x=0 \vee y=0)$ gilt, falls Null nur Null als Teiler hat. Da jeder Körper *nullteilerfrei* ist, folgt, dass der erste Formelteil den zweiten impliziert. □

12.2 Hilbertkalkül der Prädikatenlogik

12.2.1 Semantische Folgerung

Folgerung und Äquivalenz in der Prädikatenlogik sind genauso definiert wie in der Aussagenlogik. 12-11

▶ Definition
Seien Φ und Ψ Formelmengen zur gleichen Signatur. Wir schreiben

$$\Phi \models \Psi,$$

falls jedes Modell von Φ ein Modell von Ψ ist.
Wir schreiben

$$\Phi \equiv \Psi,$$

falls Φ und Ψ die gleichen Modelle besitzen.

Beispiel
Es gilt $x = y \land y = z \models x = z$, aber $x = z \not\models x = y \land y = z$.

Beispiele von Folgerungs- und Äquivalenzbeziehungen. 12-12

▶ Satz
Für alle prädikatenlogischen Formeln φ, ψ und ρ gelten:

1. $\forall x(\varphi) \models \exists x(\varphi)$
   (Spezialfallbildung)
2. $\neg\exists x(\varphi) \equiv \forall x(\neg\varphi)$
   (Dualität von All- und Existenzquantor)
3. $\forall x(\varphi) \land \forall x(\psi) \equiv \forall x(\varphi \land \psi)$
   und genauso mit $\lor$ statt $\land$ und / oder $\exists$ statt $\forall$
   (Distributivität von All- und Existenzquantor)
4. $\forall x(\forall y(\varphi)) \equiv \forall y(\forall x(\varphi))$
   und genauso mit $\exists$ statt $\forall$
   (Kommutativität von All- und Existenzquantor)
5. $\forall x(\varphi \land \rho) \equiv \forall x(\varphi) \land \rho$ *wenn x in ρ nicht frei vorkommt;*
   analog mit $\lor$ statt $\land$ und/oder $\exists$ statt $\forall$
   (Formelteile ohne Bindung können ihren Scope verlassen)

Exemplarisch ein Beweis einer der Äquivalenzen. 12-13

Beweis. Wir zeigen $\forall x(\varphi) \land \forall x(\psi) \equiv \forall x(\varphi \land \psi)$. Dazu müssen wir *zwei Richtungen* zeigen.[1]
Für die erste Richtung sei $W = (\mathcal{S}, \alpha)$ ein *Modell von* $\forall x(\varphi) \land \forall x(\psi)$.[2] Wir müssen zeigen, dass W ein *Modell von* $\forall x(\varphi \land \psi)$ ist.[3] Sei dazu ein beliebiges $u \in U$ gegeben und sei α identisch zu α', außer dass $\alpha'(x) = u$.[4] Unter diesen Voraussetzungen müssen wir zeigen, dass $(\mathcal{S}, \alpha') \models \varphi \land \psi$ gilt.[5] Nun war W ein Modell von $\forall x(\varphi) \land \forall x(\psi)$. Dann ist W ein Modell sowohl von $\forall x(\varphi)$ als auch von $\forall x(\psi)$. Dann ist aber $(\mathcal{S}, \alpha')$ sowohl ein Modell von φ als auch von ψ und foglich auch von $\varphi \land \psi$.
Für die andere Richtung sei nun $W = (\mathcal{S}, \alpha)$ ein *Modell von* $\forall x(\varphi \land \psi)$. Wir wollen *zeigen*, dass W ein *Modell von* $\forall x(\varphi) \land \forall x(\psi)$ ist.[6] Dazu genügt es zu zeigen, dass W ein Modell sowohl von $\forall x(\varphi)$ als auch von $\forall x(\psi)$ ist.[7] In beiden Fällen sei wieder ein u beliebig gewählt und $\alpha'(x) = u$ und wir wollen zeigen, dass $(\mathcal{S}, \alpha') \models \varphi$ und $(\mathcal{S}, \alpha') \models \psi$ gelten. Beides folgt daraus, dass $(\mathcal{S}, \alpha') \models \varphi \land \psi$ gilt. □

Kommentare zum Beweis

[1] Hinweis auf das verwendete Beweisrezept
[2] Beweisrezept »All-Aussagen beweisen«
[3] Vorsichtshalber das Ziel nochmal hingeschrieben.
[4] Nach Definition des All-Quantors ist dies genau die Situation, die wir analysieren müssen
[5] Bis hierher wurden eigentlich nur Namen eingeführt und der Beweis »geplant«. Jetzt kommen die eigentlichen Argumente.
[6] Vorbereitungen der zweiten Richtung abgeschlossen.
[7] Das genügt, denn dann ist es auch ein Modell von deren Konjunktion.

✎ Zur Übung 12-14
Welche der folgenden Behauptungen stimmen?

1. »$\varphi \equiv \psi$« bedeutet, dass φ und ψ genau dieselben Modelle besitzen.
2. »$\varphi \equiv \psi$« bedeutet, dass φ ein Modell von ψ ist und auch ψ ein Modell von φ ist.
3. $\varphi \land \psi \equiv \psi \land \varphi$
4. $\varphi \to \psi \equiv \psi \to \varphi$

12.2.2 Wiederholung: Beweissysteme

12-15

Wiederholung: Beweissysteme

Ein *Beweissystem* ist ein System, um *formale Beweise* aufzuschreiben. Das Beweissystem legt *Regeln* fest, wie Beweise aufgebaut sein dürfen. Die Einhaltung der Regeln muss *sehr einfach* zu überprüfen sein.

Beispiel: Beweissysteme der Aussagenlogik

- Wahrheitstafeln
- Resolutionskalkül (der Aussagenlogik)
- Hilbertkalkül (der Aussagenlogik)

Beispiel: Beweissysteme der Prädikatenlogik

- *nicht* Wahrheitstafel
- Resolutionskalkül (der Prädikatenlogik)
- Hilbertkalkül (der Prädikatenlogik)

12.2.3 Wiederholung: Hilbertkalkül

12-16

Wiederholung: Das Beweissystem »Hilbertkalkül«

▶ Definition

Sei Φ eine Menge von Formeln (nicht notwendig Tautologien). Diese nennen wir *Voraussetzungen*. Ein *Hilbertbeweis* einer Formel ψ *unter diesen Voraussetzungen* ist eine Folge von Formeln, so dass jede durch eine der folgenden Regeln gebildet wurde:

1. Die Formel ist eines der *Axiome* des Systems.
2. Die Formel ist eine der *Voraussetzungen*, also ein Element von Φ.
3. Die Formel ist durch Anwendung des *Modus ponens* auf zwei Formeln weiter vorne entstanden.

Die letzte Formel in der Reihe muss ψ sein. Wir sagen dann, ψ *lässt sich aus* Φ *ableiten* und wir schreiben $\Phi \vdash \psi$.

12-17

Wiederholung: Die Axiome und der Modus ponens

Ein Axiomensystem der Aussagenlogik

Folgende Formeln sind Axiome, wobei φ_1, φ_2 und φ_3 beliebige Formeln sind:

I $\varphi_1 \to (\varphi_2 \to \varphi_1)$
II $\bigl(\varphi_1 \to (\varphi_2 \to \varphi_3)\bigr) \to \bigl((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\bigr)$
III $(\neg\varphi_2 \to \neg\varphi_1) \to \bigl((\neg\varphi_2 \to \varphi_1) \to \varphi_2\bigr)$

Die *Regel Modus ponens* erlaubt es, aus zwei Zeilen, die φ und $\varphi \to \psi$ lauten, die neue Zeile ψ zu bilden.

Im Folgenden werden wir einfach noch *sechs weitere Axiome hinzufügen*.

12.2.4 Das Axiomensystem

12-18

Das Axiomensystem der Prädikatenlogik

Folgende Formeln sind Axiome, wobei φ_1, φ_2 und φ_3 beliebige Formeln sind, u und v Variablen und t ein Term:

I $\varphi_1 \to (\varphi_2 \to \varphi_1)$,
II $\bigl(\varphi_1 \to (\varphi_2 \to \varphi_3)\bigr) \to \bigl((\varphi_1 \to \varphi_2) \to (\varphi_1 \to \varphi_3)\bigr)$,
III $(\neg\varphi_2 \to \neg\varphi_1) \to \bigl((\neg\varphi_2 \to \varphi_1) \to \varphi_2\bigr)$,
IV $\forall v(\varphi_1) \to \varphi_1[v \hookrightarrow t]$, wenn keine in t vorkommende Variable in φ_1 gebunden vorkommt,
V $\varphi_1 \to \forall v(\varphi_1)$, wenn v nicht frei in φ_1 vorkommt,
VI $\forall v(\varphi_1 \to \varphi_2) \to (\forall v(\varphi_1) \to \forall v(\varphi_2))$,
VII $\forall u(\varphi_1[v \hookrightarrow u]) \to \forall v(\varphi_1)$, wenn u nicht in φ_1 vorkommt,
VIII $v = v$,
IX $u = v \to (\varphi_1 \to \varphi_1[u \hookrightarrow v])$, wenn φ_1 atomar ist.

Weiterhin sind auch alle obigen Formeln Axiome, wenn man ihnen beliebig Allquantoren voranstellt.
Eine Ableitung in diesem erweiterten System beschreiben wir wieder mit dem Symbol $\vdash$.

Beispiel eines Beweises. 12-19

Es gilt $x = y \vdash y = x$, wie folgender *formale Beweis* zeigt:

1. $\forall z(x = y \to (x = z \to y = z))$
   Axiom IX für u gleich x und v gleich y, ein vorangestellter Quantor
2. $\forall z(x = y \to (x = z \to y = z)) \to (x = y \to (x = x \to y = x))$
   Axiom IV für v gleich z und t gleich x
3. $x = y \to (x = x \to y = x))$
   Modus ponens auf 1 und 2
4. $x = y$
   Voraussetzung
5. $x = x \to y = x$
   Modus ponens auf 4 und 3
6. $x = x$
   Axiom VIII
7. $y = x$
   Modus ponens auf 6 und 5

12.2.5 Gödel'scher Vollständigkeitssatz

Einer der wichtigsten Sätze der Mathematik. 12-20

▶ Satz: Gödel, 1929
Das vorgestellte Beweissystem für die Prädikatenlogik ist vollständig und korrekt.

Der Satz ist ein *Spezialfall* von folgendem Satz für $\Phi = \emptyset$:

▶ Satz: Gleichheit von Folgerung und Ableitung
Sei Φ eine prädikatenlogische Formelmenge und ψ eine Formel. Dann gilt

$$\Phi \models \psi \quad \text{genau dann, wenn} \quad \Phi \vdash \psi.$$

Bemerkungen: Wie bei der Aussagenlogik gelten die beiden Sätze eigentlich nur für Formeln einer bestimmten Syntax – sie dürfen nur die Junktoren $\to$ und $\neg$ benutzen und den All-Quantor. Wie in der Aussagenlogik läßt sich dies aber leicht verallgemeinern, indem man weitere Axiome für die anderen Symbole hinzufügt.
Zum Beweis: Der Beweis geht ähnlich wie in der Aussagenlogik: Man zeigt, dass jede konsistente Formelmenge ein Modell hat. Die Hauptschwierigkeit besteht darin, dies Modell zu konstruieren. Die Details des Beweises gehen zeitlich über die Möglichkeiten dieser Einführungsvorlesung hinaus.

Zur Bedeutung des Satzes 12-21

Jeder mathematische Satz in jedem Mathematiklehrbuch *ist letztendlich eine Tautologie* der Prädikatenlogik:
Steht in einem Mathebuch *»Satz: In einem Körper gibt es keinen Nullteiler.«*, so könnte dort auch stehen: *»Satz: Die Formel* $\forall x \forall y \forall z\big((x+y)+z = x+(y+z) \wedge x+y = y+x \wedge 0+x = x \wedge \exists w(w+x = 0) \wedge (x \cdot y) \cdot z = x \cdot (y \cdot z) \wedge x \cdot y = y \cdot x \wedge 1 \cdot x = x \wedge \exists w(w \cdot x = 1) \wedge (x+y) \cdot z = (x \cdot z) + (y \cdot z)\big) \to \big(x \cdot y = 0 \to (x = 0 \vee y = 0)\big)$ *ist eine Tautologie.«* Nach dem Satz von Gödel gibt es zu jeder solchen Tautologie einen *formalen Beweis*, diesen kann man *leicht von Computern überprüfen lassen*. Man kann Beweise sogar *durch Computer finden lassen, indem einfach alle möglichen Beweise systematisch durchprobiert werden*.
Also: *Man kann ein Computerprogramm schreiben, dass bei Eingabe eines (fast) beliebigen wahren mathematischen Satzes einen Beweis für diesen Satz ausgibt.*

12.3 Syntax und Semantik der Prädikatenlogik in Kurzform

Skript-Referenz

Hier nochmal in Kurzform die komplette Syntax und Semantik der Prädikatenlogik.

Definition: Logische Signatur

Eine *(logische) Signatur* besteht aus disjunkten Mengen von Funktionssymbolen, Relationssymbolen und Konstantensymbolen, sowie einer Funktion, die jedem Funktions- und Relationssymbol eine positive natürliche Zahl zuordnet, die *Stelligkeit* genannt.

Notation

Wenn wir eine Signatur aufschreiben, so benutzen wir Großbuchstaben für die Relationssymbole und Kleinbuchstaben für die Funktions- und Konstantensymbole. Die Stelligkeiten schreiben wir als hochgestellte Indizes; Konstanten werden durch den Index 0 gekennzeichnet.

Definition: Logische Struktur

Sei σ eine Signatur. Eine logische Struktur zu dieser Signatur ist ein Tupel, bestehend aus

1. einer nichtleeren Menge U, genannt Universum,
2. einem Element $c^{\mathcal{S}} \in U$ für jedes Konstantensymbol c in σ,
3. einer Relation $R^{\mathcal{S}} \subseteq U^n$ für jedes n-stellige Relationssymbol R in σ und
4. einer Funktion $f^{\mathcal{S}}\colon U^n \to U$ für jedes n-stellige Funktionssymbolen f in σ.

Definition: Welt

Sei σ eine Signatur. Eine *(prädikatenlogische) Welt* zur Signatur σ besteht aus

1. einer logischen Struktur $\mathcal{S}$ zur Signatur σ und
2. einer Variablenbelegung $\alpha\colon \{x, x', x'', x''', \dots\} \to U$.

Definition: Syntax von Term

Sei σ eine logische Signatur. Ein Term zur Signatur σ ist ein Wort über dem Alphabet $\{x, {}', \text{Kommasymbol}, (,)\} \cup K \cup F$, wobei K die Menge der Konstantensymbole in σ ist und F die Menge der Funktionssymbole. Folgende Wörter sind Terme:

1. Jede Variable ist ein Term (also jedes Wort der Form $x'^{\cdots}{}'$).
2. Jedes Konstantensymbol in σ ist ein Term.
3. Ist f ein n-stelliges Funktionssymbol in σ und sind t_1 bis t_n Terme, so ist $f(t_1, \dots, t_n)$ ein Term.

Definition: Syntax von Formeln

Sei σ eine Signatur. Die *prädikatenlogischen Formeln* zu dieser Signatur sind Wörter über dem Alphabet $\{x, {}', (,), \forall, \exists, \wedge, \vee, \to, \leftrightarrow, =, \text{Kommasymbol}\} \cup K \cup F \cup R$, wobei K, F und R die Mengen der Konstanten-, Funktions- und Relationssymbole in σ sind. Folgende Wörter sind *atomare Formeln*:

1. $t_1 = t_2$, wobei t_1 und t_2 Terme zur Signatur σ sind.
2. $R(t_1, \dots, t_n)$, wobei R ein n-stelliges Relationssymbol ist und die t_i Terme.

Neben den atomaren Formeln sind weiterhin folgende Wörter Formeln:

3. $\neg\varphi$, wenn φ bereits eine Formel ist.
4. $(\varphi \circ \psi)$, wenn $\circ$ einer der Junktoren $\wedge$, $\vee$, $\to$ oder $\leftrightarrow$ ist und φ und ψ Formeln sind.
5. $\exists v(\varphi)$ und auch $\forall v(\varphi)$, wenn v eine Variable ist und φ eine Formel.

Definition: Substitution

Sei φ eine Formel, v eine Variable und t ein Term. Zunächst definiert man die Substitution für Terme τ:

Art des Terms τ	Substitution $\tau[v \hookrightarrow t]$
Variable v	t
Variable u (ungleich v)	u
Konstantensymbol c	c
Funktionsanwendung $f(t_1, \dots, t_n)$	$f(t_1[v \hookrightarrow t], \dots, t_n[v \hookrightarrow t])$

Nun für die Substitution für Formeln φ:

Art der Formel	Substitution $\varphi[v \hookrightarrow t]$
$t_1 = t_2$	$t_1[v \hookrightarrow t] = t_2[v \hookrightarrow t]$
$R(t_1, \dots, t_2)$	$R(t_1[v \hookrightarrow t], \dots, t_n[v \hookrightarrow t])$
$\neg\varphi$	$\neg\varphi[t \hookrightarrow v]$
$(\varphi \circ \psi)$ für Junktoren $\circ$	$(\varphi[v \hookrightarrow t] \circ \psi[v \hookrightarrow t])$
$\forall v(\varphi)$	$\forall v(\varphi)$
$\exists v(\varphi)$	$\exists v(\varphi)$
$\forall u(\varphi)$ für u ungleich v	$\forall u(\varphi[v \hookrightarrow t])$
$\exists u(\varphi)$ für u ungleich v	$\exists u(\varphi[v \hookrightarrow t])$

- Definition: Auswertung von Termen
Sei σ eine Signatur, $W = (\mathcal{S}, \alpha)$ eine Welt zu dieser Signatur und t ein Term zu dieser Signatur. Die Auswertung $\text{eval}_W(t)$ ist wie folgt rekursiv definiert:
  1. $\text{eval}_W(v) = \alpha(v)$, wobei v eine Variable ist.
  2. $\text{eval}_W(c) = c^{\mathcal{S}}$, wobei c ein Konstantensymbol ist.
  3. $\text{eval}_W\big(f(t_1, \dots, t_n)\big) = f^{\mathcal{S}}\big(\text{eval}_W(t_1), \dots, \text{eval}_W(t_n)\big)$, wobei f ein Funktionssymbol ist.

- Definition: Modellrelation
Sei σ eine Signatur, $W = (\mathcal{S}, \alpha)$ eine Welt zu dieser Signatur und φ eine Formel zu dieser Signatur. Wir schreiben $W \models \varphi$ genau in folgenden Fällen:
  1. φ hat die Form $t_1 = t_2$ und $\text{eval}_W(t_1) = \text{eval}_W(t_2)$.
  2. φ hat die Form $R(t_1, \dots, t_n)$ und $\big(\text{eval}_W(t_1), \dots, \text{eval}_W(t_n)\big) \in R^{\mathcal{S}}$.
  3. $\varphi = \neg\psi$ und es gilt nicht $W \models \psi$.
  4. $\varphi = (\psi \wedge \rho)$ und sowohl $W \models \psi$ also auch $W \models \rho$.
  5. $\varphi = (\psi \vee \rho)$ und $W \models \psi$ oder $W \models \rho$.
  6. $\varphi = (\psi \to \rho)$ und es gilt nicht sowohl $W \models \psi$ als auch $W \not\models \rho$.
  7. $\varphi = (\psi \leftrightarrow \rho)$ und es gelten entweder sowohl $W \models \psi$ als auch $W \models \rho$ oder beide gelten gerade nicht.
  8. $\varphi = \exists v(\psi)$ und es gibt ein Objekt s im Universum U von $\mathcal{S}$, so dass $W' \models \psi$ gilt, wobei $W' = (\mathcal{S}, \alpha')$ und α' unterscheidet sich von α nur dadurch, dass $\alpha'(v) = s$.
  9. $\varphi = \forall v(\psi)$ und für jedes Objekte $s \in U$ gilt $W' \models \psi$, wobei $W' = (\mathcal{S}, \alpha')$ und sich jedes α' (eines für jedes s) von α nur dadurch unterscheidet, dass $\alpha'(v) = s$.

- Definition: Modell
Sei φ eine Formel. Ein *Modell von* φ ist eine Welt W mit $W \models \varphi$. Falls φ keine freien Variablen hat, so heißt auch eine logische Struktur $\mathcal{S}$ ein *Modell von* φ, falls $(\mathcal{S}, \alpha) \models \varphi$ für irgendein α (und damit für alle α) gilt.

- Definition: Tautologie, Erfüllbarkeit, Kontradiktion
Eine Formel φ heißt eine *Tautologie*, falls jede Welt ein Modell von φ ist. Sie heißt *erfüllbar*, falls sie ein Modell hat. Sie heißt *kontradiktorisch*, falls sie kein Modell hat.

- Definition: Folgerung, Äquivalenz
Seien Φ und Ψ Formelmengen zur gleichen Signatur. Wir schreiben $\Phi \models \Psi$, falls jedes Modell von Φ ein Modell von Ψ ist. Wir schreiben $\Phi \equiv \Psi$, falls Φ und Ψ die gleichen Modelle haben.

Zusammenfassung dieses Kapitels

- Semantische Folgerung 12-22
  - Es gilt $\Phi \models \Psi$, falls jedes Modell von Φ ein Modell von Ψ ist.
  - Es gilt $\Phi \equiv \Psi$, falls Φ und Ψ dieselben Modelle haben.

- Beweissystem für die Prädikatenlogik
Es gibt ein Hilberbeweissystem für die Prädikatenlogik. Es hat neun Axiome und nutzt den Modus ponens. Wir schreiben
$$\Phi \vdash \psi,$$
falls es einen *formalen Beweis* in diesem System von ψ gibt, der neben den Axiomen die Formeln als Φ als *Voraussetzungen* nutzen darf.

- Gödel'scher Vollständigkeitssatz
$$\Phi \vdash \psi \quad \text{genau dann, wenn} \quad \Phi \models \psi.$$
Aufgrund dieses Satzes ließen sich prinzipiell *alle* mathematische Sätze *maschinell* überprüfen.

Zum Weiterlesen

[1] Norman Megill, Metamath, Lulu Press, 2007, verfügbar auf us.metamath.org.

Dieses Buch beschreibt das Metamath-Projekt. Es hat sich zur Aufgabe gemacht, eines Tages die gesamte Mathematik tatsächlich vollständig formal »aufzuschreiben« und dann maschinell zu überprüfen. Würde dieses Ziel erreicht, so gäbe es keine fehlerhaften Beweise mehr.

Übungen zu diesem Kapitel

Typische Prüfungsfragen

Die eingekreiste Zahl sind die Minuten, die für die Frage in einer Prüfung zur Verfügung stünden. Eine Prüfung besteht zu 40% aus leichten (grünen) Fragen, zu 50% aus mittleren und zu 10% aus schweren.

12 min

Prüfungsfrage 12.1

→ Lösung

Beweise führen

Zeigen Sie, dass für prädikatenlogische Formeln φ, ψ und ρ gilt:

$$\varphi \models \psi \text{ und } \varphi \models \rho \text{ genau dann, wenn } \varphi \models \psi \wedge \rho.$$

12 min

Prüfungsfrage 12.2

Beweise führen

Seien φ, ψ und ρ prädikatenlogische Formeln, wobei in ψ die Variable x nicht vorkommt. Zeigen Sie die folgenden Äquivalenzen:

1. $\exists x(\varphi) \vee \psi \equiv \exists x(\varphi \vee \psi)$
2. $\exists x(\varphi) \wedge \forall x(\rho) \equiv \exists x(\varphi \wedge \rho)$

Lösung zu 12.1

Wir behaupten, dass für beliebige prädikatenlogische Formeln φ, ψ und ρ gilt:

$$\varphi \models \psi \text{ und } \varphi \models \rho \text{ genau dann, wenn } \varphi \models \psi \wedge \rho.$$

Zum Beweis zeigen wir zwei Richtungen. Für die Richtung von links nach rechts, nehmen wir an, $\varphi \models \psi$ und $\varphi \models \rho$ gelten. Um zu zeigen, dass dann auch $\varphi \models \psi \wedge \rho$ gilt, sei W ein beliebiges Modell von φ. Wir müssen zeigen, dass W auch ein Modell von $\psi \wedge \rho$ ist. Da W ein Modell von φ ist, folgt aus den Annahmen $\varphi \models \psi$ und $\varphi \models \rho$, dass W auch ein Modell von sowohl ψ als auch von ρ ist. Per Definition ist W damit auch ein Modell von $\psi \wedge \rho$, was zu beweisen war.

Für die zweite Richtung gelte $\varphi \models \psi \wedge \rho$. Wir wollen zeigen, dass dann sowohl $\varphi \models \psi$ als auch $\varphi \models \rho$ gelten. Sei dazu W ein Modell von φ. Nach Voraussetzung ist W auch ein Modell von $\psi \wedge \rho$. Damit ist W insbesondere ein Modell sowohl von ψ als auch von ρ. Also gilt sowohl $\varphi \models \psi$ als auch $\varphi \models \rho$, was zu beweisen war.

Anhang

Referenz: Beweisrezepte

Zusammenstellung aller Beweisrezepte

Beweisrezept: *All-Aussagen beweisen* A-1

Ziel

Es soll gezeigt werden »für alle Dinge, die so und so sind, gilt blah« oder auch »jedes Ding, das so und so ist, hat die Eigenschaft blah«.

Rezept

1. Beginne den Beweis mit »Sei x ein beliebiges Ding, das so und so ist.«
2. Zeige nun, dass x die Eigenschaft blah hat.

A-2

Beweisrezept: *Beweise strukturieren*

Ziel

Der Leser soll immer genau wissen, was bereits gezeigt wurde und was noch zu zeigen ist.

Rezept

Beweise werden schnell »unübersichtlich« werden. Abhilfe:

- Benutzen Sie Wendungen wie »Damit wurde gezeigt, dass ...« oder »Es bleibt zu zeigen, dass ...« oder »Im Folgenden zeigen wir zunächst ..., ... zeigen wir hingegen später.«
- Geben Sie am Anfang eines langen Beweises eine Übersicht und teilen Sie den Beweis in Abschnitte wie »Die Konstruktion« oder »Die Rückrichtung der Korrektheit der zweiten Unterkonstruktion«.
- Formulieren Sie Zwischenbehauptung als Lemmata, die Sie zu erst beweisen.

A-3

Beweisrezept: *Details weglassen*

Ziel

Der Beweis soll kurz und knapp bleiben.

Rezept

1. Man lässt »langweilige« Teile des Beweises weg.
2. Freundlicherweise schreibt stattdessen »Man kann zeigen, dass...« oder auch »Auf den Nachweis, dass ... gilt, wurde verzichtet«.

Vermeiden sollte man »Trivialerweise gilt ...« oder »Offensichtlich gilt ...«, dies reizt den Leser eher zu argumentieren, dass dies doch nicht so trivial ist.

A-4

Beweisrezept: *Fallunterscheidung*

Ziel

Es soll gezeigt werden, dass eine beliebige Behauptung gilt.

Rezept

1. Leite den Beweis mit »Wir machen eine Fallunterscheidung.« ein.
2. Man benennt zwei oder mehr beliebige Annahmen (»Fälle« genannt), die mit der Behauptung nichts zu tun haben brauchen, von denen aber in jeder Situation mindestens (besser: genau) eine zutreffen muss.
3. Für jede Annahme X schreibt man »Fall X:«, gefolgt von einem Beweis, dass X die Behauptung impliziert.

A-5

Beweisrezept: *Induktion*

Ziel

Es soll gezeigt werden, dass eine Behauptung für $n = 1, 2, 3, \ldots$ gilt.

Rezept

1. Zeige, dass die Behauptung für $n = 1$ gilt.
   (Tipp: Hier kann man probieren, einfach »trivial« zu schreiben, das wird meistens akzeptiert.)
2. Man nimmt an, dass die Behauptung für ein vorgegebenes n gilt (aber vielleicht nicht für andere n). Man folgere, dass die Behauptung dann doch auch für $n + 1$ gilt.

Beweisrezept: *Konstruktive Beweise* A-6

Ziel
Es soll gezeigt werden, dass es ein Ding mit bestimmten Eigenschaften gibt.

Rezept
1. Man gibt an, wie ein bestimmtes Ding *konstruiert* werden soll.
2. Man zeigt nun, dass das konstruierte Ding die behaupteten Eigenschaften hat.

Der zweite Schritt wird gerne vergessen!

Beweisrezept: *Kreisschluss* A-7

Ziel
Es soll gezeigt werden, dass mehrere Behauptungen gleichwertig sind.

Rezept
Zeige, dass die Aussagen sich kreisförmig implizieren. Dies geschieht wie folgt:

1. Nimm an, dass die erste Aussage gilt. Folgere, dass nun auch die zweite gelten muss.
2. Beginne nun eine neue Argumentation. Nimm an, dass die zweite Aussage gilt. Folgere, dass dann die dritte gelten muss.
3. Und so weiter bis zur letzte, für die man zeigt, dass sie die erste impliziert.

Falls nun eine Aussage gilt, so gelten folglich alle.

Beweisrezept: *Namen für Teile vergeben* A-8

Ziel
Man möchte über die Teile eines Dings »reden«.

Rezept
1. Ist das Ding ein Tupel mit einer festen Anzahl Komponenten (wie zum Beispiel eine Grammatik, die immer aus vier Teilen besteht), so schreibt man »Sei $G = (N, T, S, E)$ eine Grammatik…« oder »Sei $G = (V, E)$ ein Graph…«.
2. Ist das Ding ein Tupel mit einer variablen Anzahl Komponenten, so schreibt man »Sei $(x_1, x_2, x_3, \dots, x_n)$ das Tupel…«. Nebenbei hat man mit n auch einen Namen für die Länge des Tupels eingeführt.
3. Ist das Ding eine abzählbare Menge, so schreibt man »Sei $M = \{m_1, m_2, m_3, \dots, m_n\}$« (bei endlichen Mengen) oder »Sei $M = \{m_1, m_2, m_3, \dots\}$« (bei abzählbar unendlichen Mengen).

Beweisrezept: *Trennung der Ebenen* A-9

Ziel
Die zwei Beweisebenen sollen dem Leser klar werden.

Rezept
1. Für die »Objekte der Logik« benutzen wir *Formeln* und *Symbole*.
2. Für die Metaebene benutzen wir *normalsprachlichen Text*.

Beispiel: Gute Schreibweise
… Falls $\hat{\beta}(\psi) = 0$, so gilt $\hat{\beta}(\psi \to \varphi) = 1$. …

Beispiel (Schlechte Schreibweise)
… $\hat{\beta}(\psi) = 0 \to \hat{\beta}(\psi \to \varphi) = 1$. …

A-10

Beweisrezept: *Wahrheitstafeln für Tautologien*

Ziel

Zeigen, dass eine Formel eine Tautologie ist.

Rezept

1. Identifiziere alle vorkommenden Variablen oder geeignete Teilformeln.
2. Für jede mögliche Kombination von Wahrheitswerten der Variablen oder Teilformeln verifiziere, dass die Formel zu wahr auswertet.

A-11

Beweisrezept: *Widerspruchsbeweis*

Ziel

Eine Behauptung beweisen, indem man zeigt, dass die Annahme des Gegenteils zu einem Widerspruch führt.

Rezept

1. Leite den Beweis mit »Wir führen einen Widerspruchsbeweis.« oder »Zum Zwecke des Widerspruchs nehmen wir an, dass XYZ nicht gilt.«
2. Führe nun einen Beweis, in dem die Annahme »nicht XYZ« beliebig benutzt werden darf.
3. Beende den Beweis, wenn doch »XYZ« hergeleitet wurde oder wenn ein offensichtlich falsche Behauptung wie $1 = 2$ hergeleitet wurde, mit »Widerspruch.« oder »Dies ist aber ein Widerspruch zur Annahme, dass nicht XYZ gilt, weshalb doch XYZ gelten muss«.

A-12

Beweisrezept: *Zwei Beweisrichtungen*

Ziel

Es soll gezeigt werden, dass eine Behauptungen A genau dann gilt, wenn eine andere Behauptung B gilt.

Rezept

Zeige, dass die Aussagen sich gegenseitig implizieren:

1. Beginne mit »Es sind zwei Richtungen zu zeigen.«
2. Fahre fort mit »Für die erste Richtung nehmen wir an, dass A gilt.« Folgere, dass dann auch B gelten muss.
3. Beginne einen neuen Absatz mit »Für die Rückrichtung nehmen wir an, dass B gilt.« Folgere, dass dann auch A gelten muss.