

Logik und formale Methoden

Vorlesungsskript

von
Burkhardt Renz

Wintersemester 2020/21

Burkhardt Renz
Technische Hochschule Mittelhessen
Rev 0.43 – 19. Oktober 2020

© 2020 by Burkhardt Renz



Dieses Dokument ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz (siehe <http://creativecommons.org/licenses/by-sa/4.0/>).

Inhaltsverzeichnis

Inhaltsverzeichnis	ii
1 Einleitung	1
1.1 Klassiker der Logik	1
1.2 Mathematische Logik	6
1.3 Logik und Informatik	11
1.4 Programm der Veranstaltung	14
I Aussagenlogik	16
2 Aussagen und Formeln	17
3 Die formale Sprache der Aussagenlogik	20
4 Die Semantik der Aussagenlogik	26
4.1 Modell, Belegung	28
4.2 Wahrheitstafel	30
4.3 Semantische Äquivalenz und Substitution	31
4.4 Boolesche Operatoren und funktionale Vollständigkeit .	32
5 Das Beweissystem des natürlichen Schließens	34
5.1 Schlussregeln	36
5.2 Beispiele für das natürliche Schließen	38
5.3 Beweisstrategien	41
5.4 Eigenschaften der Herleitbarkeit \vdash	43
5.5 Vollständigkeit des natürlichen Schließens	46
6 Normalformen	59
6.1 Negationsnormalform NNF	59
6.2 Konjunktive Normalform CNF	60
6.3 Disjunktive Normalform DNF	62
6.4 Normalformen und Entscheidungsprobleme	62
7 Die Komplexität des Erfüllbarkeitsproblems	64
7.1 Das Erfüllbarkeitsproblem	64

7.2	Komplexität von Algorithmen	65
7.3	Die Komplexität des Erfüllbarkeitsproblems	68
8	Hornlogik	70
9	Erfüllbarkeit und SAT-Solver	73
9.1	DIMACS-Format	73
9.2	Tseitin-Transformation	75
9.3	DPLL und CDLC	76
10	Anwendungen der Aussagenlogik in der Softwaretechnik	83
10.1	Anwendungen von SAT-Techniken	83
10.2	Statische Codeanalyse	84
10.3	Featuremodelle für (Software-)Produktlinien	85
II	Prädikatenlogik	89
11	Objekte und Prädikate	90
11.1	Elemente der Sprache der Prädikatenlogik	91
11.2	Prädikate und Relationen	92
12	Die formale Sprache der Prädikatenlogik	93
12.1	Signatur, Terme, Formeln	93
12.2	Freie und gebundene Variablen	95
12.3	Substitution	96
13	Semantik der Prädikatenlogik	98
13.1	Modell/Struktur	98
13.2	Semantische Folgerung und Äquivalenz	100
13.3	Fundamentale Äquivalenzen der Prädikatenlogik	101
14	Natürliches Schließen in der Prädikatenlogik	102
14.1	Schlussregeln	103
14.2	Beispiele	104
14.3	Vollständigkeit des natürlichen Schließens	105
15	Unentscheidbarkeit der Prädikatenlogik	106
16	Anwendungen der Prädikatenlogik in der Softwaretechnik	107
16.1	Analyse von Softwaremodellen mit Alloy	107
III	Lineare Temporale Logik	108
17	Dynamische Modelle	109

18 Die formale Sprache der linearen temporalen Logik (LTL)	110
19 Die Semantik der linearen temporalen Logik (LTL)	112
19.1 Kripke-Struktur	112
19.2 Äquivalenzen von Formeln der LTL	117
19.3 Typische Aussagen in der LTL	118
20 Natürliches Schließen in der LTL	119
21 Anwendungen der LTL in der Softwaretechnik	120
21.1 Model Checking	120
21.2 Zielenmodell in der Anforderungsanalyse	120
Literaturverzeichnis	121

Kapitel 1

Einleitung

Die Wissenschaft der Logik befasst sich mit den *Formen* des Denkens unter Absehen vom jeweiligen Inhalt. Es geht um das Argumentieren, das Überzeugen, um *zwingende* Schlussfolgerungen. Es ist die Wissenschaft, bei der sich das Denken gewissermaßen mit sich selbst beschäftigt. Dies kann man auf sehr unterschiedliche, auch fragwürdige Weise tun. In der *formalen Logik* geht es um ein *Kalkül*, bei dem aus gegebenen Prämissen Schlußfolgerungen gezogen werden durch die Manipulation von *Symbolen* — etwas was Computer gut können, ohne auch nur den geringsten Schimmer von der Bedeutung dieser Symbolen zu haben.

1.1 Klassiker der Logik

Ein Beispiel für eine zwingende Schlussfolgerung ist etwa folgende Argumentation über natürliche Zahlen:

$$\begin{array}{c} \text{Wenn } p > 2 \text{ und Primzahl ist, dann ist } p + 1 \text{ keine Primzahl} \\ 7 > 2 \text{ und 7 ist prim} \\ \hline \text{Also: } 7 + 1 = 8 \text{ ist keine Primzahl} \end{array}$$

Kenntnisse über natürliche Zahlen helfen, diese Argumentation zu überprüfen: Wenn die natürliche Zahl p größer als 2 und prim ist, dann muss p ungerade sein, denn sonst wäre p durch 2 teilbar, also keine Primzahl. Ist p ungerade, dann ist $p+1$ gerade, also da größer als 2 garantiert keine Primzahl. Die erste Prämisse der Argumentation ist also zutreffend. Die zweite auch — man kann ja einfach nach den echten Teilern von 7 suchen und findet nur die 1. Beide Prämissen treffen zu, die Schlussfolgerung über die Zahl 8 folglich auch, das *Also* ist gerechtfertigt.

Wenn man die folgende Schlussfolgerung betrachtet, dann hat sie strukturell denselben Aufbau:

Wenn es regnet, ist die Straße nass.
Es regnet.

Also: Die Straße ist nass.

Diese Struktur, nämlich

$$\frac{P \rightarrow Q \\ P}{\text{Also: } Q}$$

nennt man *Modus Ponens*, aus dem Lateinischen *ponere* = stellen, setzen, also der setzende Modus, die Schlussfigur, die die Aussage *Q* „setzt“.

Wir finden sie auch bei folgender Argumentation —

Wenn die Erde eine Kugel ist, dann ist 7 eine Primzahl.
Die Erde ist eine Kugel.

Also: 7 ist eine Primzahl.

— und rein formal betrachtet sind auch hier beide Prämisse zutreffend, also die Schlussfolgerung zwingend. Aber während bei dem Beispiel mit der nassen Straße ein inhaltlicher Zusammenhang der Aussagen besteht, ist dies in diesem Beispiel offensichtlich nicht der Fall. Die Aussage über die Erde und die Aussage über die Zahl 7 schließen sozusagen *windschief* aneinander vorbei. Anders gesagt: Die rein formale Betrachtung hat auch ihren Preis, reichlich *unsinnige* Aussagen werden als zutreffend erachtet. In der Symbiose von formaler Logik und Informatik spielt dies allerdings keine Rolle, denn die Systeme, die die Informatik baut (und sie selbst) sind *selbst* formale Systeme.

Die Beobachtung, dass man die *formale Struktur* von Argumentationen ohne Kenntnisse der Inhalte betrachten und sie als zwingende *Schlussregel* sehen kann, hat vielleicht als erster Aristoteles¹ gemacht. Er hat *Syllogismen* (als dem Altgriechischen für „Zusammenrechnen“, „logischer Schluss“) betrachtet:

Eine Deduktion (*syllogismos*) ist also ein Argument, in welchem sich, wenn etwas gesetzt wurde, etwas anderes als das Gesetzte mit Notwendigkeit durch das Gesetzte ergibt.

– Aristoteles: Topik I 1, 100a25-27

¹ Aristoteles, griechischer Philosoph, 384 - 322 v. Chr.

Die Syllogismen haben immer zwei Prämisse und eine Konklusion. Ein oft zitiertes Beispiel ist:

Alle Menschen sind sterblich.
Alle Griechen sind Menschen.

Also: Alle Griechen sind sterblich.

Dieser Syllogismus wird *Modus Barbara* genannt, weil er von zwei All-Aussagen zu einer Schlussfolgerung führt, die auch eine All-Aussage ist.

Aus der Perspektive von Aristoteles ergeben sich Fragen wie:

- Was sind *gültige* Schlussregeln?
- Was ist ein *Beweis*?
- Wann ist eine Theorie *widerspruchsfrei*?
- ...

Man kann die Syllogismen als eine frühe Variante der Prädikatenlogik mit unären Prädikaten sehen. Erst 1879 hat Gottlob Frege² in seiner „Begriffsschrift“ die Prädikatenlogik formalisiert und damit die Grundlage gelegt für die heutige formale Logik.

Aristoteles betont im obigen Zitat, dass in einem Syllogismus die Schlussfolgerung mit *Notwendigkeit* aus den Prämissen folgt. Dies zeichnet ja gerade die Logik aus, wie in folgendem Zitat auch Goethe³ sie charakterisiert:

Mephistopheles:

Erklärt Euch, eh Ihr weiter geht,
Was wählt Ihr für eine Fakultät?

Schüler:

Ich wünschte recht gelehrt zu werden,
Und möchte gern, was auf der Erden
Und in dem Himmel ist, erfassen,
Die Wissenschaft und die Natur.

Mephistopheles:

Da seid Ihr auf der rechten Spur;
Doch müßt Ihr Euch nicht zerstreuen lassen.

Schüler:

Ich bin dabei mit Seel und Leib;

²Gottlob Frege, deutscher Logiker, Mathematiker und Philosoph, 1848 - 1925.

³Johann Wolfgang von Goethe, deutscher Dichter, 1749 - 1832

Doch freilich würde mir behagen
Ein wenig Freiheit und Zeitvertreib
An schönen Sommerfeiertagen.

Mephistopheles:

Gebraucht der Zeit, sie geht so schnell von hinten,

Doch Ordnung lehrt Euch Zeit gewinnen.

Mein teurer Freund, ich rat Euch drum

Zuerst Collegium Logicum.

Da wird der Geist Euch wohl dressiert,

In spanische Stiefeln eingeschnürt,

Daß er bedächtiger so fortan

Hinschleiche die Gedankenbahn,

Und nicht etwa, die Kreuz und Quer,

Irrlichteliere hin und her.

Dann lehret man Euch manchen Tag,

Daß, was Ihr sonst auf einen Schlag

Getrieben, wie Essen und Trinken frei,

Eins! Zwei! Drei! dazu nötig sei.

Zwar ist's mit der Gedankenfabrik

Wie mit einem Weber-Meisterstück,

Wo ein Tritt tausend Fäden regt,

Die Schifflein herüber hinüber schießen,

Die Fäden ungesehen fließen,

Ein Schlag tausend Verbindungen schlägt.

Der Philosoph, der tritt herein

Und beweist Euch, es müßt so sein:

Das Erst wär so, das Zweite so,

Und drum das Dritt und Vierte so;

Und wenn das Erst und Zweit nicht wär,

Das Dritt und Viert wär nimmermehr.

Das preisen die Schüler allerorten,

Sind aber keine Weber geworden.

Wer will was Lebendigs erkennen und beschreiben,

Sucht erst den Geist heraus zu treiben,

Dann hat er die Teile in seiner Hand,

Fehlt, leider! nur das geistige Band.

– Goethe: Faust - Der Tragödie erster Teil, Vers 1896 ff.

Goethe betont die Strenge, das Normative, das *Zwingende* der Logik — und betrauert das ebenso: ihm fehlt dabei das Lebendige und das „geistige Band“!

Auch Hegel⁴ hat einen Einwand gegen die Sichtweise des formalen Schlie-

⁴Georg Wilhelm Friedrich Hegel, deutscher Philosoph, 1770 - 1831.

ßens:

Es ist überhaupt eine bloß subjektive Reflexion, welche die Beziehung der Terminorum in abgesonderte Prämissen und einen davon verschiedenen Schlußsatz trennt:

Alle Menschen sind sterblich,
Cajus ist ein Mensch,
Also ist er sterblich.

Man wird sogleich von Langeweile befallen, wenn man einen solchen Schluß heranziehen hört; – dies röhrt von jener unnützen Form her, die einen Schein von Verschiedenheit durch die abgesonderten Sätze gibt, der sich in der Sache selbst sogleich auflöst. Das Schließen erscheint vornehmlich durch diese subjektive Gestaltung als ein subjektiver *Notbehelf*, zu dem die Vernunft oder der Verstand da ihre Zuflucht nehme, wo sie nicht *unmittelbar* erkennen könne.

– Hegel: Logik II, Werke Bd. 6, S.358

Formales Schließen in der Form eines Aristotelischen Syllogismus erscheint Hegel als „langweilig“, weil man gewissermaßen als Schlussfolgerung nur herausbekommt, was man bereits sowieso in die Prämissen hineingesteckt hat. Für ihn ist es nur der *Schein* der Verschiedenheit der Aussagen, der die Trivialität des Schlusses ausmacht.

Hegel selbst interessiert in seiner Logik etwas anderes: Er analysiert die Leistungen des Denken im „Allgemeinen“: Was sagt jemand, wenn er sagt, dass *A* die *Bedingung* für *B* ist? Was bedeutet es, *A* als *Grund* für *B* zu bezeichnen? Was macht das *Wesen* eines untersuchten Gegenstandes aus? Allgemein: wie geht das Denken im Begreifen einer Sache vor?

Zwei Perspektiven auf Logik

Ein erstes Fazit dieses schnellen (und etwas eklektizistischen) Blicks auf Klassiker der Logik ist, dass man Logik durchaus unterschiedlich sehen kann:

- **Erste Perspektive** Logik als *Gesetze des Denkens* im Sinne von (begründeten) *Normen* für korrekte Schlussfolgerungen und Argumentationen
- **Zweite Perspektive** Logik als *Gesetze des Denkens* im Sinne von „wie geht Denken?“

Wir werden bei der Betrachtung der Logik in der mathematischen Argumentation noch eine weitere Sichtweise kennenlernen.

1.2 Mathematische Logik

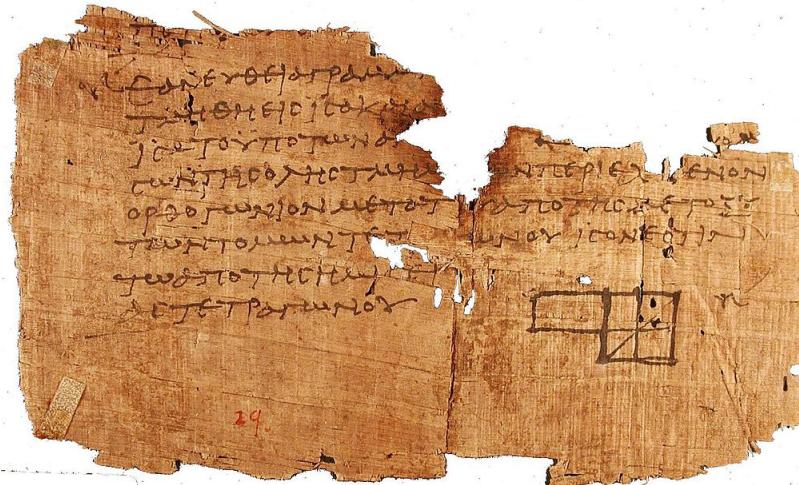


Abbildung 1.1: Papyrusfragment der „Elemente“ des Euklid

Abbildung 1.1 zeigt ein Papyrusfragment der „Elemente“ des Euklid⁵, ein Werk, das nicht nur die Geometrie als Wissenschaft begründet hat, sondern auch die Denk- und Argumentationsweise der Mathematik, die *axiomatische Methode*.

Euklid hat seine Untersuchung der Geometrie begründet auf fünf Postulate (heute würde man dazu Axiome sagen), aus denen er dann mit einigen wenigen Schlussregeln alle seine Sätze über die Geometrie herleitet. Euklid hat außerdem Definitionen der Begriffe Punkt, Gerade usw. seinen Postulaten vorangestellt. Heute werden in der Mathematik solche Grundbegriffe nicht definiert, sondern sie ergeben sich aus ihren Eigenschaften, die durch die Axiome festgelegt sind.

Die Axiome von Euklid sind:

1. Zu jedem Paar von Punkten gibt es genau eine Gerade, die durch diese Punkte geht.
2. Eine beliebige Strecke kann man zu einer Geraden verlängern.
3. Zu jedem Mittelpunkt und Radius kann man einen Kreis ziehen.
4. Alle rechten Winkel sind einander gleich.
5. Zu jeder Geraden und einem Punkt außerhalb dieser Geraden gibt es genau *eine* parallele Gerade durch diesen Punkt.

⁵Euklid von Alexandria, griechischer Mathematiker, 3. Jahrhundert v. Chr.

Was wird man von den Axiomen erwarten?

- *Widerspruchsfreiheit*: Aus den Axiomen soll sich der Widerspruch nicht herleiten lassen, denn sonst würde ja *alles* aus den Axiomen folgen!
- *Unabhängigkeit*: Es soll nicht möglich sein, ein Axiom aus den anderen zu deduzieren. Diese Frage hat sich insbesondere bezüglich des fünften Axioms von Euklid, dem Parallelenaxiom gestellt. Der Versuch, es aus den anderen Axiomen herzuleiten, hat zu interessanten Entdeckungen geführt, die wir gleich kennenlernen werden.
- *Vollständigkeit*: Ein Axiomensystem ist vollständig, wenn man alle Sätze, die man auf Basis der Terme des Systems formulieren kann, entweder beweisen oder widerlegen kann. Euklids Axiomensystem ist übrigens nicht vollständig. David Hilbert⁶ hat 1899 in seiner Schrift „Grundlagen der Geometrie“ ein vollständiges Axiomensystem für die euklidische Geometrie entworfen.

Es ist nicht gelungen, das Parallelenaxiom aus den anderen Axiomen herzuleiten. Beim Versuch dies zu tun, wurde entdeckt, dass man durch Abwandlung des Parallelenaxioms neue interessante, sogenannte nicht-euklidische Geometrien definieren kann.

Euklidische Geometrie (der Ebene) Zu einer Geraden und einem Punkte außerhalb dieser Geraden, gibt es genau *eine* Parallelle. In dieser Geometrie ist die Summe der Winkel eines Dreiecks gerade 180° .

Elliptische Geometrie (auf der Kugeloberfläche) In dieser Geometrie sind die Geraden gerade die Großkreise. Und es gilt: Zu einer Geraden und einem Punkt außerhalb derselben, gibt es *keine* Parallelle, d.h. verschiedene Geraden schneiden sich immer. In dieser Geometrie ist die Summe der Winkel eines Eulerschen Dreiecks immer größer als 180° . Abbildung 1.3 zeigt die Geraden a, b und C und das Eulersche Dreieck, das sie bilden.

Hyperbolische Geometrie In dieser Geometrie gibt es zu einer Geraden und einem Punkt außerhalb dieser Geraden *mindestens zwei* parallele Geraden. Es sind dann tatsächlich unendlich viele. Die Summe der Winkel im Dreieck ist immer kleiner als 180° .

Ein Modell der hyperbolischen Geometrie ist die Geometrie auf der offenen oberen Halbebene der Ebene, das Poincaré'sche Halbebenenmodell.

⁶David Hilbert, deutscher Mathematiker, 1862 - 1943.

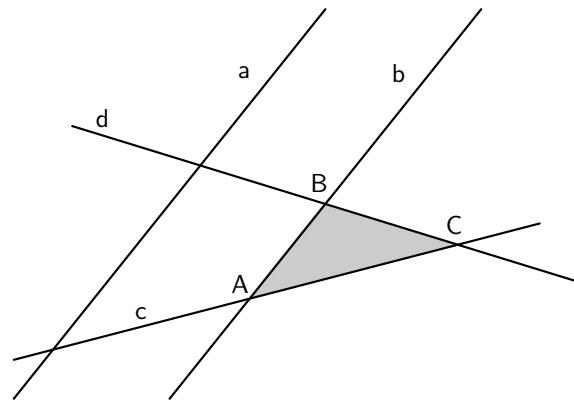


Abbildung 1.2: Euklidische Geometrie

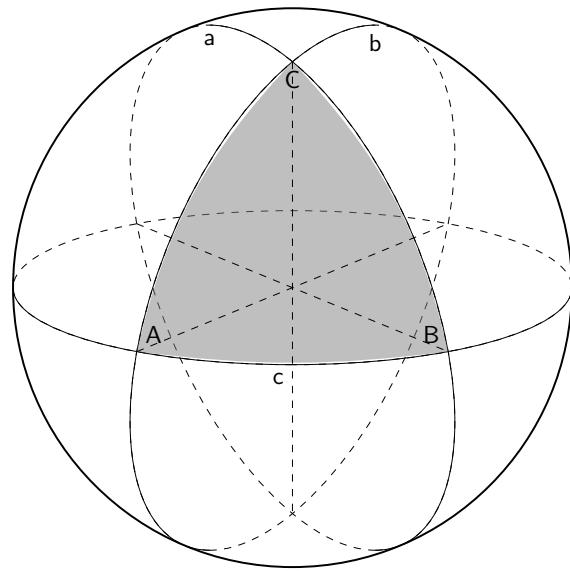


Abbildung 1.3: Elliptische Geometrie

Die Geraden sind Halbkreise oder senkrechte Halbgeraden in der offenen oberen Halbebene. In Abbildung 1.4 sind die Geraden a und b asymptotisch parallel, d.h. sie treffen sich auf der Grenze der Halbebene in einem sogenannten uneigentlichen Punkt, der nicht mehr zum Inneren der Halbebene gehört. a und c sind auch parallel, man sagt: ultraparallel, während b und c nicht parallel sind.

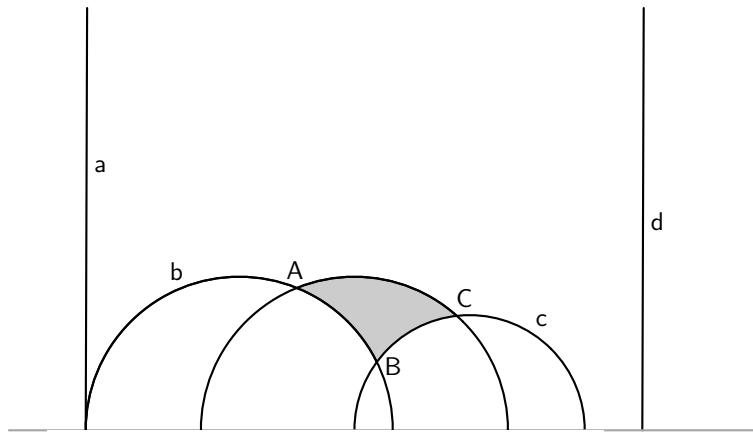


Abbildung 1.4: Hyperbolische Geometrie (Poincarés Halbebenen-Modell)

Theorie und Modell

In der mathematischen Logik hat sich (ausgehend von der Entdeckung nichteuklidischer Geometrien) eine Sprechweise von *Modell* durchgesetzt, die nicht verwechselt werden sollte mit dem Begriff des Modells, wie er zum Beispiel beim Softwaredesign mit der UML verwendet wird.

Im Beispiel der hyperbolischen Geometrie ist der Ausgangspunkt ein Axiomensystem und die Poincaré'sche Halbebene ist eine Struktur, in der sich die Terme des Axiomensystems interpretieren lassen und in der die Axiome zutreffen. Es gibt für das Axiomensystem der hyperbolischen Geometrie auch andere Modelle, zum Beispiel die Sattelfläche. Abbildung 1.5 zeigt ein Dreieck auf der Sattelfläche.

Ein *Modell* einer *Theorie* ist in der mathematischen Logik also eine mit passenden Strukturen versehene Menge, auf die die Axiome und alle daraus ableitbaren Sätze der Theorie zutreffen. Es ist wichtig, diese Denk- und Sprechweise zu kennen, denn in Teil II der Veranstaltung wird ein *Model Finder* vorkommen und in Teil III geht es u.a. um *Model Checking* — beide Bezeichnungen kommen von der Sprechweise der mathematischen Logik.

Nebenbei bemerkt: es mag einem durch diese Sprechweise die Mathematik erscheinen wie ein Spiel mit willkürlich festgelegten Regeln, den

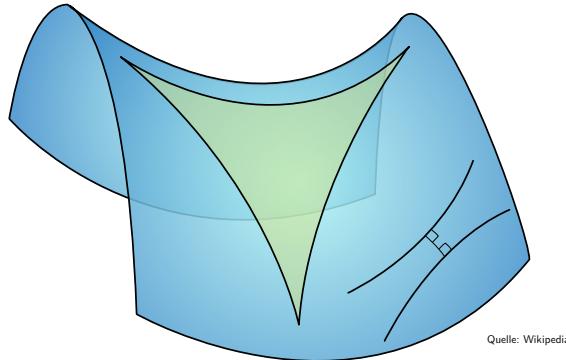


Abbildung 1.5: Hyperbolische Geometrie (Sattelfläche)

Axiomen, für die sich, sofern widerspruchsfrei, schon eine passende Wirklichkeit, ein Modell wird finden lassen. Ganz so ist es nicht. Die Axiome zu finden ist die Aufgabe, einen Sachverhalt auf seinen ganz grundlegenden Kern zu reduzieren. Natürlich kann man auch mit Variationen der Axiome „spielen“, oft führt das zu gar nichts, manchmal eröffnet es neue Einsichten.

Seine Axiomatisierung der Geometrie schien für David Hilbert das Vorbild dafür zu sein, wie Mathematik zu denken habe. Die Mathematik sollte auf die Grundlage eines Axiomensystems gestellt werden, aus der die gesamte Mathematik mit definierten und als korrekt angesehenen Schlussregeln in Beweisen mit endlich vielen Schritten hergeleitet könnte.

Wir erörtern noch kurz, welche berechtigten allgemeinen Forderungen an die Lösung eines mathematischen Problems zu stellen sind: ich meine vor Allem, die, daß es gelingt, die Richtigkeit der Antwort durch eine endliche Anzahl von Schlüssen darzuthun und zwar auf Grund einer endlichen Anzahl von Voraussetzungen, welche in der Problemstellung liegen und die jedesmal genau zu formuliren sind. Diese Forderung der logischen Deduktion mittelst einer endlichen Anzahl von Schlüssen ist nichts anderes als die Forderung der Strenge in der Beweisführung.

– David Hilbert: Vortrag auf dem internationalen Mathematiker-Kongress Paris 1900

Dritte Perspektive auf die Logik

Man kann die bisherigen Erläuterungen so zusammenfassen: Wir betrachten Logik als eine formale Sprache, deren *Syntax* präzise und eindeutig definiert ist. Die *Semantik* der Symbole der Sprache ergibt sich durch Modelle der Sprache. Und ein *Beweissystem* mit Axiomen und Schlussregeln erlaubt es durch rein symbolische Manipulation von Ausdrücken der Sprache neue Formeln herzuleiten.

- **Dritte Perspektive** Logik als *Kalkül* einer formalen Sprache — Syntax, Semantik und Beweissystem.

Und mit dieser dritten Perspektive sind wir nun schon gleich beim Thema Logik und Informatik. Denn mit formalen Sprachen und Umformungen von Ausdrücken kennt sich die Informatik ja bestens aus. Doch bevor wir auf falsche Ideen kommen, lassen wir noch Henri Poincaré⁷ zu Wort kommen:

Wer einer Schachpartie beiwohnt, dem wird es zum Verständnis der Partie nicht genügen, die Regeln über den Lauf der Figuren zu kennen. Was würde ihm nur erlauben zu erkennen, daß jeder Zug den Regeln entsprechend gespielt wurde, und dieser Vorzug hätte sehr wenig Wert. Es wäre jedoch das gleiche, wie es dem Leser eines mathematischen Buches ginge, wenn er nur Logiker wäre. Die Partie verstehen, das ist etwas ganz anderes, das heißt wissen, warum der Spieler mit dieser Figur zieht anstatt mit jener anderen, was er auch hätte tun können, ohne die Spielregeln zu übertreten; das heißt den inneren Grund zu erkennen, der aus dieser Reihe aufeinanderfolgender Züge ein organisches Ganzes macht. Mit viel mehr Grund ist diese Fähigkeit dem Spieler selbst nötig, das heißt dem Erfinder.

— Henri Poincaré: Der Wert der Wissenschaft, S.15

1.3 Logik und Informatik

[Symbolic] Logic and computer science share a symbiotic relationship. Computers provide a concrete setting for the implementation of logic. Logic provides language and methods for the study of theoretical computer science.

— Shawn Hedman: A First Course in Logic, S.xiv

⁷Henri Poincaré, französischer Mathematiker, 1854 - 1912.

Diese enge Beziehung zwischen formaler Logik und Informatik zeigt sich in vielen Teilgebieten der Informatik, etwa:

Digitaltechnik

Kombinatorische Schaltungen implementieren logische Operatoren. In der Digitaltechnik als einem Teilgebiet der technischen Informatik spielt also die Aussagenlogik eine ganz grundlegende Rolle.

Komplexitätstheorie

In diesem Teilgebiet der Informatik geht es um die Komplexität algorithmisch behandelbarer Probleme, insbesondere was die Rechenzeit in Abhängigkeit von der Größe der Eingabe angeht. In der Komplexitätstheorie ist die Frage immer noch ungeklärt, ob effizient verifizierbare Probleme (der Klasse \mathcal{NP}) sich auch in polynomieller Zeit lösen lassen, also auch in der Klasse \mathcal{P} sind. Ein oder vielleicht das Musterbeispiel für ein Problem der Klasse \mathcal{NP} ist das Problem der Erfüllbarkeit einer Formel der Aussagenlogik.

Datenbanken

Relationale Datenbanken kann man sehen als endliche Modelle von Sprachen der Prädikatenlogik. Datenbankabfragen kann man deshalb auch in Formeln der Prädikatenlogik übersetzen. Man kann vereinfacht sagen, dass heutiges SQL als Sprache die Ausdrucksmächtigkeit der Prädikatenlogik mit transitivem Abschluss hat. Die Solidität relationaler Datenbanksysteme ist sicherlich auch darauf zurückzuführen, dass mit der relationalen Algebra, die auf der Prädikatenlogik basiert, eine mathematische Grundlage existiert.

Logik und Softwaretechnik

In dieser Veranstaltung interessieren wir uns aber insbesondere für den Zusammenhang zwischen Logik und Softwaretechnik.

A specification is a written description of what a system is supposed to do. Specifying a system helps us understand it.
It's a good idea to understand a system before building it, so it's a good idea to write a specification of a system before implementing it.

...

Our basic tools for writing specifications is mathematics. Mathematics is nature's way of letting you know how sloppy your writing is. It's hard to be precise in an imprecise language like English or Chinese. In engineering, imprecision

can lead to errors. To avoid errors, science and engineering have adopted mathematics as their language.

– Leslie Lamport: Specifying Systems, S.1f.⁸

Da wir mit einem Computerprogramm letztlich eine formale Beschreibung des Verhaltens einer abstrakten Maschine formulieren, müssen wir in der Softwaretechnik im Grunde den Beweis erbringen, dass diese Beschreibung die Anforderungen an das Programm tatsächlich erfüllt.

A solution of the problem [of providing a software based machine to fulfill a purpose in the real world, i.e. software development] must be based on at least the following descriptions:

- **requirement \mathcal{R} :** a statement of the customer's requirement;
- **domain properties \mathcal{W} :** a description of the given properties of the problem world;
- **specification \mathcal{S} :** a specification of the machine's behaviour at its interface with the problem world; and
- **program \mathcal{P} :** a program describing the machine's internal and external behaviour in a language that the general-purpose computer can interpret.

To show that the problem is solved we must discharge a proof obligation whose form is, roughly:

$$(\mathcal{P} \Rightarrow \mathcal{S}) \wedge ((\mathcal{S} \wedge \mathcal{W}) \Rightarrow \mathcal{R})$$

– Michael Jackson: Where, Exactly, Is Software Development? LNCS 2757, 2003⁹

Man kann das auch etwas plakativ ausdrücken (im folgenden Zitat steht S für Spezifikation, E für Environment — bei Jackson die Domain Properties und R für Requirements):

... the more we realised the key role of the fundamental logic—that $S, E \vdash R$ is truly the $E = mc^2$ of requirements engineering.

– Anthony Hall: $E = mc^2$ Explained, 2010¹⁰

⁸Leslie Lamport, amerikanischer Informatiker. Mehr zum Thema Spezifikation in Leslie Lamparts Vortrag *Thinking for Programmers*, URL: <http://channel9.msdn.com/Events/Build/2014/3-642>.

⁹Michael Jackson (not the singer), britischer Informatiker, geb. 1936.

¹⁰Anthony Hall, britischer Informatiker.

1.4 Programm der Veranstaltung

Viele Fragestellungen in der Softwaretechnik und der Programmierung haben eine Darstellung in der *Aussagenlogik*, die wir im ersten Teil der Veranstaltung behandeln werden. Ein Beispiel ist die Beherrschung der Variabilität in Softwareproduktlinien, für die Featuremodelle eingesetzt werden, bei deren Analyse Techniken des *SAT-Solving*, der Lösung des Erfüllbarkeitsproblems der Aussagenlogik, zum Einsatz kommen.

Man kann sich auch fragen, ob Spezifikationen widerspruchsfrei sind, ob sie gewünschte Eigenschaften tatsächlich erfüllen, oder ob sich Gegenbeispiele finden lassen. Wir werden im zweiten Teil der Veranstaltung nach der Diskussion der *Prädikatenlogik* als Werkzeug die Sprache *Alloy* und den *Alloy Analyzer* kennenlernen, mit dem man leichtgewichtig und interaktiv Mikromodelle von Architekturen, Entwürfen, Software überprüfen kann.

Man kann auch so vorgehen, dass man gebaute oder konzipierte Softwaresysteme logisch exakt beschreibt und dann prüft, ob sie gewünschte Eigenschaften tatsächlich erfüllen. Die Modelle sind häufig dynamische Modelle und die gewünschten Eigenschaften werden als Formeln der *linearen temporalen Logik (LTL)* formuliert. Mit der Technik des *Model Checking* kann man insbesondere in verteilten Systemen beweisbar überprüfen, ob Eigenschaften etwa der Fairness, des wechselseitigen Ausschlusses und Ähnliches erfüllt sind.

Wir werden also drei Logiken behandeln und jeweils einen Blick auf Anwendungen in der Softwareentwicklung werfen:

1. Aussagenlogik
2. Prädikatenlogik
3. Lineare temporale Logik

Dabei wird bei der Diskussion der Grundlagen die oben skizzierte dritte Perspektive auf die Logik verwendet, d.h.

- Die formale Sprache der jeweiligen Logik, also die *Syntax*
- Die *Semantik* der jeweiligen Logik, also Modelle in denen die Ausdrücke der formalen Sprache repräsentiert werden können
- Ein *Beweissystem*, das es erlaubt aus gegebenen Formeln durch Umformungen nach gewissen Regeln andere Formeln herzuleiten, und damit Beweise zu führen. Es gibt verschiedene solche Beweissysteme. Wir werden das Beweissystem des *natürlichen Schließens* in allen drei Logiken verwenden. Das natürliche Schließen kann

auch durch Software unterstützt werden, eine Software, die die jeweiligen Schritte bei der Anwendung der Regeln überprüft. Die *Logic Workbench lwb*¹¹ ist ein solches Werkzeug, das das natürliche Schließen in allen drei Logiken unterstützt.

¹¹Wiki zu Natural Deduction mit lwb auf github.

Teil I

Aussagenlogik

Kapitel 2

Aussagen und Formeln

In der Aussagenlogik werden Aussagen betrachtet, die wahr oder falsch sein können. Solche Aussagen nennt man *wahrheitsdefinite* Aussagen. Es gibt viele andere Formen von Aussagen in natürlichen Sprachen, wie z.B. ironische Äußerungen, Fragen oder Aufforderungen. Die Sprache der Aussagenlogik ist eine *formale* Sprache, in der nur wahrheitsdefinite Aussagen verwendet werden.

Beispiele

$P =$ „Göttingen ist nördlich von Frankfurt“

$Q =$ „6 ist eine Primzahl“

$R =$ „Jede gerade Zahl > 2 ist die Summe zweier Primzahlen“¹

aber nicht:

„Könnten Sie bitte die Türe schließen“, eine Aufforderung

„Wie spät ist es“, eine Frage

„Guten Tag“, ein Gruß

Der *Inhalt* der Aussagen ist für die Aussagenlogik nicht wirklich von Belang. Wir studieren *nicht* den Wahrheitsgehalt von Aussagen, sondern die *Beziehung* der Aussagen.

Wir können atomare Aussagen miteinander verbinden und daraus zusammengesetzte Aussagen, *Formeln* bilden. Die Verbindung wird durch *Junktoren* hergestellt - siehe Tabelle 2.1

Mit Junktoren können wir Aussagen verbinden.

¹ Goldbach-Vermutung, benannt nach dem Mathematiker Christian Goldbach (1690 - 1764).

Tabelle 2.1: Junktoren und weitere Symbole

\neg	„nicht“, not	Negation
\wedge	„und“, and	Konjunktion
\vee	„oder“, or	Disjunktion
\rightarrow	„impliziert“, implies	Implikation
\top	„wahr“, true , verum	Wahrheit
\perp	„falsch“, false , absurdum	Widerspruch

Beispiele

- $P \wedge Q$ „Göttingen ist nördlich von Frankfurt *und* 6 ist eine Primzahl“ ①
- $P \vee Q$ „Göttingen ist nördlich von Frankfurt *oder* 6 ist eine Primzahl“ ②
- $P \rightarrow Q$ „Göttingen ist nördlich von Frankfurt *impliziert* 6 ist eine Primzahl“ ③
- $Q \rightarrow P$ „6 ist eine Primzahl *impliziert* Göttingen ist nördlich von Frankfurt“ ④

Bemerkungen

1. Die erste Aussage ist falsch. Allerdings muss man bei der Übertragung von Aussagen aus der natürlichen Sprache Vorsicht walten lassen:
Die folgenden beiden Aussagen haben einen unterschiedlichen Sinn
„Er ging zur Schule und ihm war langweilig.“
„Ihm war langweilig und er ging zur Schule.“
obwohl die Aussagen $P \wedge Q$ und $Q \wedge P$ in der formalen Sprache der Aussagenlogik äquivalent sind.
2. Die zweite Aussage ist wahr.
3. Die dritte Aussage ist falsch.
4. Die vierte Aussage ist wahr – obwohl offensichtlicher Unsinn! Implikationen in der formalen Logik darf man nicht mit *Kausalität* verwechseln. Die Aussage ist wahr, weil in der formalen Logik das Prinzip *ex falso quodlibet* gilt: Aus einer falschen Voraussetzung darf man alles folgern. Warum diese Definition der Implikation sinnvoll ist, werden wir später sehen.
5. Es gibt Aussagen, die wahr sind, egal welche Wahrheitswerte die beteiligten atomaren Aussagen haben, wie z.B.
 $((P \rightarrow Q) \rightarrow (\neg P \vee Q)) \wedge ((\neg P \vee Q) \rightarrow (P \rightarrow Q))$
Solche Aussagen nennt man allgemeingültig oder *Tautologie*.

Wir haben in dieser einführenden Diskussion zwei Konzepte verwendet, ohne sie genau zu unterscheiden: Die *Syntax* der Aussagenlogik, die festlegt, welche Formeln wir aus atomaren Aussagen und Junktoren bilden können, sowie die *Semantik* der Aussagenlogik, bei der wir von Wahrheitswerten der atomaren Aussagen reden und aus diesen den Wahrheitswert von Formeln ermitteln können.

In den folgenden drei Kapiteln werden wir diese beiden Konzepte und ihren Zusammenhang auf systematische Weise untersuchen.

Kapitel 3

Die formale Sprache der Aussagenlogik

In der Sprache der Aussagenlogik kombiniert man atomare Aussagen mit Junktoren. Dabei gehen wir von einer gegebenen Menge \mathcal{P} von Aussagensymbolen sowie Junktoren aus. Genau genommen beziehen sich die folgenden Definitionen auf die Wahl dieser Menge und man sollte von *einer* Sprache der Aussagenlogik sprechen.

Definition 3.1 (Alphabet der Aussagenlogik). Das *Alphabet* der Sprache der Aussagenlogik besteht aus

- (i) einer Menge \mathcal{P} von Aussagensymbolen,
- (ii) den Junktoren: $\neg, \wedge, \vee, \rightarrow$
- (iii) der Konstanten: \perp
- (iv) den zusätzlichen Symbolen: $(,)$

Bemerkungen

- Für eine Sprache der Aussagenlogik nennt man die Wahl der Menge der Aussagensymbole sowie der Junktoren usw. auch die *logische Signatur*.
- Viele Autoren geben eine fixe (abzählbare) Menge von Aussagensymbolen vor, etwa $\mathcal{P} = \{P_0, P_1, P_2, \dots\}$ und sprechen dann von *der* Sprache der Aussagenlogik.¹

¹Die Menge der Aussagensymbole muss übrigens nicht unbedingt abzählbar sein, sondern kann eine beliebige Menge sein, siehe [Rau08, S. 4 und Abschnitt 1.5]. Das ist interessant, wenn man den Kompaktheitssatz der Aussagenlogik verwendet, um Aussagen über unendliche Mengen zu beweisen. In dieser Vorlesung werden wir uns damit nicht befassen, weil wir uns auf Anwendungen der formalen Logik in Informatik und Softwaretechnik konzentrieren.

Für Anwendungen der Aussagenlogik in der Informatik und der Softwareentwicklung haben wir jedoch mit endlichen Mengen zu tun und wir möchten den Aussagensymbole auch „sprechende“ Bezeichnungen geben können. Deshalb geht in unsere Definition des Alphabets die Wahl der Menge der Aussagensymbole ein.

- Die Bezeichnung von \neg, \wedge etc. als *Junktoren* soll unterstreichen, dass wir eine formale Sprache definieren. Natürlich aber darf man schon daran denken, dass mit \neg die *Negation* („nicht“), mit \wedge die *Konjunktion* („und“), mit \vee die *Disjunktion* („oder“) und mit \rightarrow die *Implikation* („impliziert“) gemeint sind.
- Die Konstante \perp steht für den *Widerspruch* („falsch“).
- Auch was die Junktoren angeht, treffen wir in der Definition eine Wahl. Wir könnten z.B. noch weitere Junktoren hinzunehmen, wie etwa \leftrightarrow oder auch Junktoren weglassen. Wir werden später sehen, dass sich aus der Semantik der Aussagenlogik ergibt, dass die Menge von Operatoren, die unsere gewählten Junktoren definieren *funktional vollständig* ist, d.h. jede beliebige Boolesche Funktion darstellen kann.

Definition 3.2 (Formeln der Aussagenlogik). Die *Formeln* der Aussagenlogik sind Zeichenketten, die nach folgenden Regeln gebildet werden:

- (i) Jedes Aussagensymbol ist eine Formel und auch \perp ist eine Formel.
- (ii) Ist ϕ eine Formel, dann auch $(\neg\phi)$.
- (iii) Sind ϕ und ψ Formeln, dann auch $(\phi \wedge \psi)$, $(\phi \vee \psi)$ und $(\phi \rightarrow \psi)$

Bemerkungen

- In der Definition der Formeln der Aussagenlogik verwenden wir auch die Implikation, wenn wir z.B. sagen: „Ist ϕ eine Formel, dann auch $(\neg\phi)$ “. Man muss also unterscheiden, ob wir *über* die Logik sprechen — man sagt dann auch: wir verwenden die *Metasprache* — oder ob wir eine logische Formel angeben — dann verwenden wir die *Objektsprache*, die wir eben definiert haben.
- Die Symbole ϕ und ψ sind also *Variablen der Metasprache*, sie stehen als Platzhalter für *Formeln der Objektsprache*.
- Unsere Definition der Menge der Formeln der Aussagenlogik ist eine sogenannte *induktive* Definition.
- Eine Formel, die nur aus einem Aussagensymbol oder \perp besteht, nennt man auch *atomare* Formel oder *Primformel*.

Als *Grammatik* in Backus-Naur-Darstellung² können wir diese induktive Definition der Formeln der Aussagenlogik so ausdrücken:

$$\phi ::= P \mid \perp \mid (\neg\phi) \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \rightarrow \phi)$$

mit Aussagensymbolen $P \in \mathcal{P}$ und (bereits gebildeten) Formeln ϕ .

Zu einer Formel ϕ kann man ihren Syntaxbaum bilden:

Definition 3.3. Als *Syntaxbaum* bezeichnen wir einen endlichen Baum, dessen Knoten mit Formeln beschriftet sind und der folgende Eigenschaften hat:

- (i) Die Blätter sind mit Primformeln beschriftet.
- (ii) Ist ein Knoten mit einer Formel der Form $(\neg\phi)$ beschriftet, dann hat er genau ein Kind, das mit ϕ beschriftet ist.
- (iii) Ist ein Knoten mit einer Formel der Form $(\phi \wedge \psi)$, $(\phi \vee \psi)$ oder $(\phi \rightarrow \psi)$ beschriftet, dann hat er genau zwei Kinder und das linke ist mit ϕ , das rechte mit ψ beschriftet.

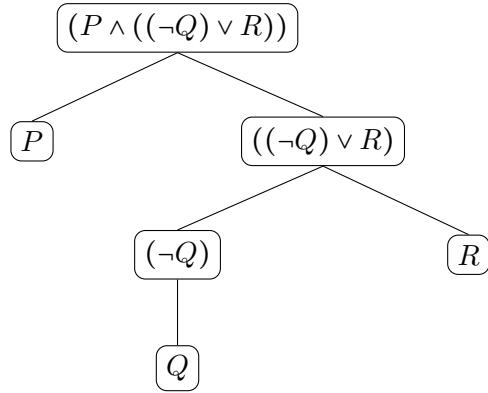
Ein Syntaxbaum repräsentiert die Formel, mit der die Wurzel des Baumes beschriftet ist.

Beispiel 3.1. Gegeben sei die Formel

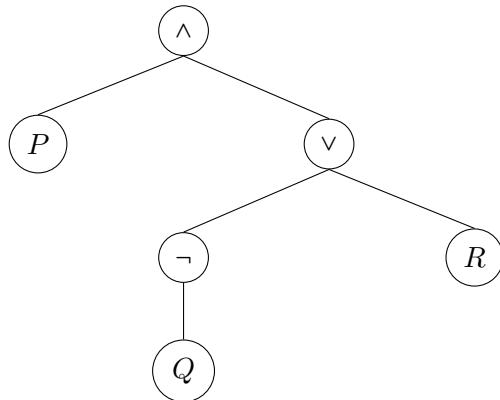
$$(P \wedge ((\neg Q) \vee R))$$

Der Syntaxbaum ist dann

²John W. Backus, amerikanischer Informatiker, 1942 - 2007; Peter Naur, dänischer Informatiker, 1928 - 2016 (Tatsächlich war Naur nicht erfreut über diese Bezeichnung, er hätte „Backus-Normalform“ vorgezogen.)



Wir verwenden oft die abgekürzte Darstellung des Syntaxbaums, in der die Knoten nicht mit den Subformeln bezeichnet werden, sondern mit dem Operator. Nur an den Blättern des Baums kommen dann die Primformeln vor. In unserem Beispiel also



Bemerkung Die Sprechweise „*der* Syntaxbaum einer Formel“ unterstellt, dass es nur *einen* solchen Baum zu einer gegebenen Formel gibt. Mit anderen Worten: die Grammatik aus der Definition der Formeln ist eindeutig.

Satz 3.1. *Jede Formel der Aussagenlogik hat genau einen Syntaxbaum.*

Zum Beweis von Aussagen über Formeln wendet man oft das Prinzip der *strukturellen Induktion* an.

Prinzip der strukturellen Induktion Sei \mathcal{E} eine Eigenschaft. Dann gilt $\mathcal{E}(\phi)$ für alle Formeln ϕ , wenn gilt:

- (i) \mathcal{E} gilt für alle Primformeln und \perp .
- (ii) Gilt \mathcal{E} für ϕ , dann auch für $(\neg\phi)$.
- (iii) Gilt \mathcal{E} für ϕ und ψ , dann auch für $(\phi \wedge \psi)$, $(\phi \vee \psi)$ und $(\phi \rightarrow \psi)$.

Dieses Prinzip kann man anwenden, um obigen Satz zu beweisen.

Beweisidee für Satz 3.1. Man beweist den Satz in folgenden Schritten:
Zunächst zeigt man: Jede Formel hat eine gerade Anzahl von Klammern und zwar ebenso viele öffnende wie schließende Klammern.

Dann zeigt man: Jedes echte Anfangsstück einer Formel hat mehr öffnende als schließende Klammern.

Mit Hilfe dieser beiden Aussagen kann man dann den Satz beweisen. \square

Definition 3.4 (Subformel). Eine *Subformel* einer Formel ϕ ist eine Formel, die als Beschriftung an einem Knoten des Syntaxbaums von ϕ vorkommt.

Definition 3.5 (Rang einer Formel). Der *Rang* $\text{rg}(\phi)$ einer Formel ist definiert durch

- (i) $\text{rg}(\phi) = 0$, wenn ϕ eine Primformel.
- (ii) $\text{rg}((\phi \square \psi)) = \max(\text{rg}(\phi), \text{rg}(\psi)) + 1$, wobei \square für einen der Junktoren $\wedge, \vee, \rightarrow$ steht.
- (iii) $\text{rg}((\neg\phi)) = \text{rg}(\phi) + 1$.

Der Rang einer Formel ist gerade die Tiefe des Syntaxbaums, d.h. die maximale Pfadlänge von der Wurzel zu einem beliebigen Blatt.

Die Eindeutigkeit des Syntaxbaums erlaubt es uns, Konventionen zu vereinbaren, mit denen man Klammern „sparen“ kann. Man vereinbart, dass die Junktoren in folgender Reihenfolge binden, die stärkste Bindung zuerst: $\neg, \wedge, \vee, \rightarrow$. Außerdem sind \wedge und \vee linksassoziativ; \rightarrow ist rechtsassoziativ.

Bemerkung Für die Definition der Syntax der Aussagenlogik haben wir die *Infix-Notation* verwendet, wie das in den Lehrbüchern über formale Logik üblich ist.

Man kann stattdessen die *Präfix-Notation* verwenden und hat dann folgende Grammatik:

$$\phi ::= P \mid \perp \mid (\neg \phi) \mid (\wedge \phi \dots) \mid (\vee \phi \dots) \mid (\rightarrow \phi \phi)$$

In der Präfix-Notation kann man die Junktoren \wedge und \vee als *n-äre* Junktoren definieren.

In der [Logic Workbench \(lwb\)](#), einer in Clojure geschriebenen Bibliothek von Funktionen für die Aussagen-, Prädikaten- und lineare temporale Logik wird Präfix-Notation mit folgenden Junktoren verwendet:

Tabelle 3.1: Junktoren für die Aussagenlogik in lwb

Junktor	Beschreibung	Arität
<code>not</code>	Negation	unär
<code>and</code>	Konjunktion	n-är
<code>or</code>	Disjunktion	n-är
<code>impl</code>	Implikation	binär
<code>equiv</code>	Äquivalenz	binär
<code>xor</code>	Exklusives Oder	binär
<code>ite</code>	If-then-else	ternär

Beispiel 3.2. Die Formel

$$(P \wedge ((\neg Q) \vee R))$$

in Infix-Notation wird in der Präfix-Notation der Logic Workbench so geschrieben:

```
(and P (or (not Q) R))
```

Diese Schreibweise entspricht genau dem Syntaxbaum der Formel.

Kapitel 4

Die Semantik der Aussagenlogik

In der klassischen Aussagenlogik wird jedem Aussagensymbol ein Wahrheitswert aus der Menge $\{T, F\}$ zugeordnet. (T steht für `true` und F für `false`, viele Autoren verwenden auch die Menge $\{1, 0\}$).

Die Bedeutung einer Formel der Aussagenlogik ergibt sich dann daraus, dass man diese Zuordnung von den Aussagensymbolen auf die Formel erweitert, in dem man definiert, welcher Wahrheitswert sich beim Zusammensetzen von Formeln durch die Junktoren ergibt. Auf diese Weise definiert man den Booleschen *Operator* zum jeweiligen Junktor.

Bemerkung Die Festlegung auf genau zwei Wahrheitswerte definiert eine *zweiwertige* Logik. Man kann auch andere Festlegungen treffen wie:

- Łukasiewic¹-Logik mit den Wahrheitswerten $\{1, \frac{1}{2}, 0\}$ oder $\{T, U, F\}$. Łukasiewic² versteht den Wert $\frac{1}{2}$ als „nicht bewiesen, aber auch nicht widerlegt“, manchmal wird der dritte Wert U auch als „unbekannt“ interpretiert, wie zum Beispiel in SQL.
- Zadeh²-Logik mit Wahrheitswerten im Intervall $[0, 1]$; eine Logik mit dieser Semantik wird auch Fuzzy-Logik genannt.

Sei $\mathbb{B} = \{T, F\}$. Die Junktoren $\neg, \wedge, \vee, \rightarrow$ können als *Operatoren* auf der Menge \mathbb{B} , also als Boolesche Operatoren aufgefasst werden, in dem man die Verknüpfungstafeln wie folgt definiert:

¹Jan Łukasiewic², polnischer Philosoph, Mathematiker und Logiker 1878 - 1956.

²Lotfi A. Zadeh, amerikanischer Informatiker, 1921 - 2017

	ϕ	$\neg\phi$
\neg	T	F
	F	T

$\neg\phi$ genau dann **true**, wenn ϕ **false**.

	ϕ	ψ	$\phi \wedge \psi$
\wedge	T	T	T
	T	F	F
	F	T	F
	F	F	F

$\phi \wedge \psi$ ist genau dann **true**, wenn sowohl ϕ als auch ψ **true** sind.

	ϕ	ψ	$\phi \vee \psi$
\vee	T	T	T
	T	F	T
	F	T	T
	F	F	F

$\phi \vee \psi$ ist genau dann **true**, wenn einer der Operanden **true** ist. \vee ist also ein einschließendes oder.

	ϕ	ψ	$\phi \rightarrow \psi$
\rightarrow	T	T	T
	T	F	F
	F	T	T
	F	F	T

Bemerkung

Der Operator \rightarrow wird auch als *materiale Implikation*³ bezeichnet. Er behauptet *keinen* kausalen Zusammenhang zwischen der linken Seite, dem *Antezedens* und der rechten Seite, der *Konsequenz* oder dem *Sukzedens*.

Es seien die Aussagen

$$\begin{aligned} P &= \text{„Die Erde umkreist die Sonne“}, \\ P' &= \text{„Die Sonne umkreist die Erde“ und} \\ Q &= \text{„6 ist Primzahl“} \end{aligned}$$

gegeben.

$P \rightarrow Q$ hat den Wahrheitswert F – wie man vielleicht erwarten würde, auch wenn kein inhaltlicher Zusammenhang zwischen den beiden Aussagen besteht.

Hingegen hat $P' \rightarrow Q$ den Wahrheitswert T – denn das Antezedens ist F. Das kann man vielleicht so interpretieren: „Wenn die Sonne um die Erde kreisen würde, dann wäre 6 eine Primzahl“ – und da ja die Sonne nicht um die Erde kreist, können wir über die 6 sagen, was wir wollen.

³nach Bertrand Russell und Alfred North Whitehead: *Principia Mathematica* (1910).

Dahinter steckt ein klassisches logisches Prinzip: *ex falso quodlibet*⁴ – „aus Falschem folgt alles, was beliebt“.

Der für uns wichtigere Grund für die Verwendung der materiellen Implikation ist jedoch, dass man mit dieser Definition der Implikation eine *einfache* Logik bekommt – in der zum Beispiel folgender Sachverhalt einfach ausdrückbar ist:

Die Aussage $\forall x \in \mathbb{N} : (x > 3) \rightarrow (x > 1)$ ist T.

Setze ein:

$x = 4$	$(4 > 3) \rightarrow (4 > 1)$	Ergebnis
	T T	T
$x = 2$	$(2 > 3) \rightarrow (2 > 1)$	Ergebnis
	F T	T
$x = 0$	$(0 > 3) \rightarrow (0 > 1)$	Ergebnis
	F F	T

In allen drei Fällen ist die Aussage true.

Die materielle Implikation führt zu sogenannten Paradoxien, z.B.

- (1) $P \rightarrow (Q \rightarrow P)$ ist allgemeingültig
„Wenn P gilt, folgt P aus allem“.
- (2) $\neg P \rightarrow (P \rightarrow Q)$ ist allgemeingültig
„Wenn P nicht gilt, dann folgt alles aus P “.

4.1 Modell, Belegung

Sei \mathcal{P} die Menge der Aussagensymbole und \mathbb{B} die Menge der Wahrheitswerte.

Definition 4.1. Eine Abbildung $v : \mathcal{P} \rightarrow \mathbb{B}$ nennt man ein *Modell* für die Sprache der Aussagenlogik. Man nennt Modelle der Aussagenlogik auch spezifischer *Belegung*, weil durch v jedem Aussagensymbol ein Wahrheitswert zugewiesen wird.

Definition 4.2. Zu einem Modell $v : \mathcal{P} \rightarrow \mathbb{B}$ und einer Formel ϕ definiert man den Wahrheitswert $\llbracket \phi \rrbracket_v \in \mathbb{B}$ der Formel induktiv durch

⁴eigentlich „ex falso sequitur quodlibet“.

- (i) $\llbracket P \rrbracket_v := v(P)$ für alle $P \in \mathcal{P}$
- (ii) $\llbracket \perp \rrbracket_v := \text{F}$
- (iii) $\llbracket (\neg\phi) \rrbracket_v := \begin{cases} \text{T falls } \llbracket \phi \rrbracket_v = \text{F} \\ \text{F sonst} \end{cases}$
- (iv) $\llbracket (\phi \wedge \psi) \rrbracket_v := \begin{cases} \text{T falls } \llbracket \phi \rrbracket_v = \text{T und } \llbracket \psi \rrbracket_v = \text{T} \\ \text{F sonst} \end{cases}$
- (v) $\llbracket (\phi \vee \psi) \rrbracket_v := \begin{cases} \text{T falls } \llbracket \phi \rrbracket_v = \text{T oder } \llbracket \psi \rrbracket_v = \text{T} \\ \text{F sonst} \end{cases}$
- (vi) $\llbracket (\phi \rightarrow \psi) \rrbracket_v := \begin{cases} \text{T falls } \llbracket \phi \rrbracket_v = \text{F oder } \llbracket \psi \rrbracket_v = \text{T} \\ \text{F sonst} \end{cases}$

Bemerkung Sei ϕ eine Formel und v_1, v_2 seien Modelle mit $v_1(P) = v_2(P)$ für alle Aussagensymbole P in ϕ . Dann gilt:

$$\llbracket \phi \rrbracket_{v_1} = \llbracket \phi \rrbracket_{v_2}.$$

Man kann sich zu einer gegebenen Belegung v fragen, welchen Wahrheitswert eine Formel ϕ hat. Diese Frage ist einfach zu beantworten, indem man die Formel auswertet. Spannender ist die „umgekehrte“ Fragestellung: Gegeben ein Formel ϕ , gibt es dann eine Belegung, in der die Formel T ist, und wenn ja, welche? Diese ist die Frage nach der *Erfüllbarkeit* der Formel.

Definition 4.3 (Erfüllbarkeit). Eine Formel ϕ heißt *erfüllbar*, wenn es ein Modell v gibt mit $\llbracket \phi \rrbracket_v = \text{T}$.

Definition 4.4 (Falsifizierbarkeit). Eine Formel ϕ heißt *falsifizierbar*, wenn es ein Modell v gibt mit $\llbracket \phi \rrbracket_v = \text{F}$.

Definition 4.5 (Allgemeingültigkeit). Eine Formel ϕ heißt *allgemeingültig*, wenn für alle Modelle v gilt: $\llbracket \phi \rrbracket_v = \text{T}$.

Man schreibt dann $\models \phi$ und nennt ϕ eine *Tautologie*.

Definition 4.6 (Unerfüllbarkeit). Eine Formel ϕ heißt *unerfüllbar*, wenn für alle Modelle v gilt: $\llbracket \phi \rrbracket_v = \text{F}$.

Man schreibt dann $\not\models \phi$ und nennt ϕ eine *Kontradiktion*.

Etwas salopp kann man diese Definitionen so auffassen:

- Eine Formel ist erfüllbar, wenn es eine „Welt“ gibt, in der sie wahr ist.
- Eine Formel ist falsifizierbar, wenn es eine „Welt“ gibt, in der sie nicht wahr ist.
- Eine Formel ist allgemeingültig, wenn sie in jeder möglichen „Welt“ wahr ist.
- Eine Formel ist unerfüllbar, wenn sie in keiner aller möglichen „Welt“ wahr ist.

Satz 4.1 (Dualitätsprinzip). *Eine Formel ϕ ist genau dann allgemeingültig, wenn $\neg\phi$ unerfüllbar ist.*

Beweis. Sei ϕ allgemeingültig, d.h. für alle Belegungen v gilt $\llbracket \phi \rrbracket_v = T$, d.h. aber auch dass für alle v gilt $\llbracket \neg\phi \rrbracket_v = F$, d.h. $\neg\phi$ ist unerfüllbar. Und da $\phi \equiv \neg\neg\phi$ gilt auch die Umkehrung. \square

erfüllbar			
ϕ	ψ	$\neg\psi$	$\neg\phi$
allgemeingültig	erfüllbar, nicht allgemeingültig		unerfüllbar
falsifizierbar			

Abbildung 4.1: Dualitätsprinzip

4.2 Wahrheitstafel

Um zu prüfen, ob eine Formel allgemeingültig oder erfüllbar ist, kann man die Wahrheitstafel verwenden. Im Prinzip listet man in der Wahrheitstafel alle möglichen Belegungen der Aussagensymbole in der Formel auf und berechnet in jeder dieser „Welten“ den Wahrheitswert der Formel. Man geht dabei so vor:

1. Man ermittelt die Menge der Aussagensymbole der Formel. Für jede mögliche Belegung eines Symbols mit einem Wahrheitswert bildet man eine Zeile der Wahrheitstafel. Hat die Formel n verschiedene Aussagensymbole, hat die Wahrheitstafel also 2^n Zeilen. Jedes Symbol bekommt eine Spalte der Wahrheitstabelle.

- Man bildet eine weitere Spalte der Wahrheitstafel, die mit der Formel beschriftet ist. In dieser Spalte überträgt man nun für jedes Symbol die Belegung der jeweiligen Zeile. Dann geht man entsprechend des zugehörigen Syntaxbaums von unten nach oben und ermittelt sukzessive die Wahrheitswerte der Subformeln, bis man beim Wahrheitswert der Formel angelangt ist.

Satz 4.2. *Die Methode des Aufstellens der Wahrheitstafel ist ein Entscheidungsverfahren für das Erfüllbarkeitsproblem und für das Gültigkeitsproblem.*

Beweis. Eine Formel ϕ ist *erfüllbar*, wenn es in der Wahrheitstafel *mindestens eine* Zeile mit dem Ergebnis T gibt.

Eine Formel ϕ ist *allgemeingültig*, wenn in der Wahrheitstafel *alle* Zeilen das Ergebnis T haben. \square

4.3 Semantische Äquivalenz und Substitution

Definition 4.7 (Semantische Äquivalenz). Zwei Formeln ϕ und ψ sind *semantisch äquivalent*, geschrieben $\phi \equiv \psi$, wenn für alle Belegungen v gilt: $\llbracket \phi \rrbracket_v = \llbracket \psi \rrbracket_v$.

Definition 4.8 (Logische Konsequenz). Sei Γ eine Menge von Formeln. Eine Formel ϕ heißt *logische Konsequenz* von Γ , geschrieben $\Gamma \vDash \phi$, wenn für alle Modelle v gilt:

Ist $\llbracket \gamma \rrbracket_v = T$ für alle $\gamma \in \Gamma$, dann ist auch $\llbracket \phi \rrbracket_v = T$.

Definition 4.9 (Substitution). Sei ϕ eine Subformel von ψ und ϕ' eine beliebige Formel. Dann ist $\psi[\phi'/\phi]$ (lese: ψ mit ϕ' an Stelle von ϕ) die Formel, die man erhält, wenn man jedes Vorkommen von ϕ in ψ durch ϕ' ersetzt (substituiert).

Satz 4.3 (Substitutionssatz). *Sei ϕ eine Subformel von ψ und ϕ' eine semantisch äquivalente Formel, d.h. $\phi \equiv \phi'$, dann gilt:*

$$\psi \equiv \psi[\phi'/\phi].$$

\square

Wichtige semantische Äquivalenzen

Assoziativität

$$(\phi \vee \psi) \vee \chi \equiv \phi \vee (\psi \vee \chi)$$

$$(\phi \wedge \psi) \wedge \chi \equiv \phi \wedge (\psi \wedge \chi)$$

Kommutativität

$$\phi \vee \psi \equiv \psi \vee \phi$$

$$\phi \wedge \psi \equiv \psi \wedge \phi$$

Distributivitat

$$\begin{aligned}\phi \vee (\psi \wedge \chi) &\equiv (\phi \vee \psi) \wedge (\phi \vee \chi) \\ \phi \wedge (\psi \vee \chi) &\equiv (\phi \wedge \psi) \vee (\phi \wedge \chi)\end{aligned}$$

De Morgans Gesetze

$$\begin{aligned}\neg(\phi \vee \psi) &\equiv \neg\psi \wedge \neg\phi \\ \neg(\phi \wedge \psi) &\equiv \neg\psi \vee \neg\phi\end{aligned}$$

Idempotenz

$$\begin{aligned}\phi \vee \phi &\equiv \phi \\ \phi \wedge \phi &\equiv \phi\end{aligned}$$

Doppelte Negation

$$\neg\neg\phi \equiv \phi$$

Komplement

$$\begin{aligned}\phi \wedge \neg\phi &\equiv \perp \\ \phi \vee \neg\phi &\equiv \top\end{aligned}$$

Identitatsgesetze

$$\begin{aligned}\phi \wedge \top &\equiv \phi \\ \phi \vee \perp &\equiv \phi\end{aligned}$$

Absorption

$$\begin{aligned}\phi \wedge (\phi \vee \psi) &\equiv \phi \\ \phi \vee (\phi \wedge \psi) &\equiv \phi\end{aligned}$$

Bemerkung Betrachtet man die Menge der Formeln der Aussagenlogik und bildet die Menge der Äquivalenzklassen bezüglich der semantischen Äquivalenz (\equiv), dann sagen obige Aussagen unter anderem, dass diese Menge eine *Boolesche Algebra* ist.

4.4 Boolesche Operatoren und funktionale Vollstandigkeit

Die Anzahl der unären Operatoren auf \mathbb{B} ist 4, die der binären Operatoren ist 16. Allgemein gilt:

Satz 4.4. Für $n \in \mathbb{N}$ gibt es 2^{2^n} n -äre Boolesche Operatoren.

Beweis. Hat der Operator n Argumente, dann gibt es 2^n n -Tupel von möglichen verschiedenen Werten für die Argumente. Jede dieser Kombinationen kann als Ergebnis des Operators einen der beiden Wahrheitswerte T oder F haben, also gibt es 2^{2^n} Möglichkeiten. \square

Übung:

Erstellen Sie Tabellen für alle möglichen unären und binären Operatoren, finden Sie in der Literatur die gängigen Bezeichnungen und Symbole für die Operatoren.

Offenbar kann man Operatoren durch andere Operatoren ausdrücken, z.B.

$$\phi \leftrightarrow \psi \equiv (\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$$

oder

$$\phi \rightarrow \psi \equiv \neg\phi \vee \psi$$

oder

$$\phi \wedge \psi \equiv \neg(\neg\phi \vee \neg\psi)$$

Definition 4.10. Eine Menge Boolescher Operatoren heißt *funktional vollständig*, wenn man jeden beliebigen Operator durch diese Operatoren logisch äquivalent ausdrücken kann.

Satz 4.5. Für jeden n -ären Booleschen Operator gibt es eine äquivalente Formel, die nur die Operatoren \neg und \vee hat. D.h. $\{\neg, \vee\}$ ist funktional vollständig.

Übung:

Beweisen Sie diesen Satz. Hinweis: Sehen Sie in das Skript von R. Stärk.

Kapitel 5

Das Beweissystem des natürlichen Schließens

Mit der Wahrheitstafel gibt es eine einfache Möglichkeit, festzustellen, ob eine Formel der Aussagenlogik erfüllbar ist. Man stellt die Wahrheitstafel auf und prüft, ob es eine Zeile mit dem Ergebnis T gibt.

Es gibt jedoch Beispiele, an denen man leicht sieht, dass diese Methode ihre Probleme hat. Nehmen wir etwa als Beispiel die folgende Formel:

$$(P_1 \wedge (P_1 \rightarrow P_2) \wedge \cdots \wedge (P_{n-1} \rightarrow P_n)) \rightarrow P_n$$

Diese Formel hat n Atome, die Wahrheitstafel also 2^n Zeilen.

Wir können jedoch auf eine andere Weise zu einer Lösung kommen. Wenn wir akzeptieren, dass die Schlussregel (man nennt sie *Modus ponens*)

$$\frac{\phi \quad \phi \rightarrow \psi}{\psi}$$

erlaubt ist, dann kann man so argumentieren:

P_1 und $P_1 \rightarrow P_2$ sind gegeben, also gilt P_2 .

P_2 und $P_2 \rightarrow P_3$ sind gegeben, also gilt P_3 .

...

P_{n-1} und $P_{n-1} \rightarrow P_n$ sind gegeben, also gilt P_n .

Und aus dieser Argumentation folgt, dass es sich bei der gegebenen Formel um eine Tautologie handelt.

In diesem Beispiel haben wir eine Schlussregel angewandt. Wichtig ist dabei zu sehen, dass sich damit die Perspektive gewandelt hat. In der Ermittlung der Wahrheitstafel wird die *Semantik* der Aussagenlogik verwendet: für jedes mögliche Modell, jede mögliche Belegung wird der Wahrheitswert der Formel ermittelt. In der Argumentation mit der obigen Schlussregel wird kein Bezug auf die Semantik genommen, sondern die Schlussregel wird verwendet, um Transformation an den Symbolen vorzunehmen, die die Formel ausmachen.

Sei $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$ eine Menge von Formeln und ϕ eine Formel, dann gibt es zwei Sichten auf die Frage, ob ϕ aus Γ folgt:

- *Semantische Sicht*

$$\Gamma \vDash \phi$$

In allen Modellen (allen „möglichen Welten“), in denen $\gamma_1, \gamma_2, \dots, \gamma_n$ gelten, ist auch ϕ wahr.

- *Syntaktische Sicht*

$$\Gamma \vdash \phi$$

Man kann aus den gegebenen Formeln $\gamma_1, \gamma_2, \dots, \gamma_n$ die Formel ϕ herleiten, indem man ausschließlich die Regel des Beweissystems verwendet.

Es gibt für die Aussagenlogik (und für die Prädikatenlogik) verschiedene solcher Beweissysteme. Wir werden uns in der Veranstaltung mit dem *natürlichen Schließen* (auch *natürliche Deduktion*) befassen.

Das Kalkül des natürlichen Schließen wurde 1934 von Gerhard Gentzen¹ und unabhängig von ihm von Stanisław Jaśkowski² entwickelt.

Die Bezeichnung „Natürliches Schließen“ röhrt daher, dass die Regeln des Kalküls das „natürliche“ Argumentieren von Mathematikern formalisieren.

¹Gerhard Gentzen (1909–1945) deutscher Mathematiker und Logiker, [Gen35].

²Stanisław Jaśkowski (1906–1965), polnischer Logiker.

„Mein erster Gesichtspunkt war folgender: Die Formalisierung des logischen Schließens, wie sie insbesondere durch Frege, Russell und Hilbert entwickelt worden ist, entfernt sich ziemlich weit von der Art des Schließens, wie sie in Wirklichkeit bei mathematischen Beweisen geübt wird. [...] Ich wollte nun zunächst einmal einen Formalismus aufstellen, der dem wirklichen Schließen möglichst nahekommt. So ergab sich ein ‚Kalkül des natürlichen Schließens‘“ [Gen35, S. 176].

5.1 Schlussregeln

Für die Herleitung von Formeln gibt es im natürlichen Schließen pro logischem Symbol zwei Regeln:

- eine, die das Symbol einführt (*Introduction*, abgekürzt durch i) und
- eine zweite, die das Symbol entfernt (*Elimination* auch: Auflösung), abgekürzt durch e).

Jede Regel gibt an, was *gegeben* sein muss (oberhalb des Strichs), damit die Umformung gemacht werden darf, also was sich aus dem Gegebenen *ergibt* (unterhalb des Strichs).

5.1.1 Konjunktion

Die Regeln für die Konjunktion sind:

	<i>Einführung</i>	<i>Elimination</i>
\wedge	$\frac{\phi \quad \psi}{\phi \wedge \psi}$ $\wedge i$	$\frac{\phi \wedge \psi}{\phi}$ $\wedge e_1$ $\frac{\phi \wedge \psi}{\psi}$ $\wedge e_2$

Die Konjunktion kann man einführen, wenn man Herleitungen für die beiden Formeln der Konjunktion bereits hat.

Für die Elimination der Konjunktion gibt es zwei Subregeln: Eine Herleitung der Gesamtformel der Konjunktion kann man sowohl als Herleitung der linken Teilformel als auch der rechten Teilformel nehmen.

5.1.2 Disjunktion

Die Regeln für die Disjunktion sind:

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{\phi}{\phi \vee \psi} \quad \text{vi}_1$ $\frac{\psi}{\phi \vee \psi} \quad \text{vi}_2$	$\frac{\begin{array}{c c} \phi & \psi \\ \vdots & \vdots \\ \chi & \chi \end{array}}{\chi} \quad \text{ve}$

Wenn man eine Herleitung für ϕ hat, hat man auch eine Herleitung für $\phi \vee \psi$, ebenso darf man die Herleitung von ψ als Beweis für $\phi \vee \psi$ nehmen.

Will man die Disjunktion entfernen und dabei χ herleiten, muss man für jede Teilformel der Disjunktion eine Herleitung von χ finden. Diese Regel entspricht also der Beweistechnik der Fallunterscheidung.

5.1.3 Implikation

Die Regeln für die Implikation sind:

	<i>Einführung</i>	<i>Elimination</i>
\rightarrow	$\frac{\begin{array}{c} \phi \\ \vdots \\ \psi \end{array}}{\phi \rightarrow \psi} \quad \rightarrow i$	$\frac{\phi \quad \phi \rightarrow \psi}{\psi} \quad \rightarrow e, MP$

Die Implikation leitet man her, indem man die Hypothese als gegeben annimmt und dann daraus die Folgerung herleitet. In der Regel wird in der Box oberhalb des Strichs angegeben, dass ϕ nur *innerhalb* der Box als gegeben angenommen werden darf. Die senkrechten Punkte $:$ markieren die Beweisverpflichtung, nämlich dass sie durch einen Beweis ersetzt werden müssen, der ψ aus ϕ herleitet.

Die Implikation kann man entfernen, wenn man die Hypothese ϕ bewiesen hat und ebenso, dass $\phi \rightarrow \psi$ gilt. Dann hat man ψ bewiesen. Diese Schlussfigur ist schon seit der Antike geläufig und wird als *Modus ponens* bezeichnet, deshalb auch die Abkürzung **MP**.

5.1.4 Negation

	<i>Einführung</i>	<i>Elimination</i>
\neg	$\begin{array}{c} \phi \\ \vdots \\ \perp \end{array}$	$\frac{\phi \quad \neg\phi}{\psi} \neg e, EFQ$

Will man beweisen, dass $\neg\phi$ gilt — also die Negation einführen —, nimmt man an, dass ϕ bewiesen ist und führt diesen Beweis dann fort, bis man den Widerspruch \perp hergeleitet hat. Daraus ergibt sich, dass $\neg\phi$ bewiesen ist.

5.1.5 Widerspruchsbeweis, EFQ

	<i>Einführung</i>	<i>Elimination</i>
RAA, \perp	$\begin{array}{c} \neg\phi \\ \vdots \\ \perp \end{array}$	$\frac{\perp}{\phi} \perp e, EFQ$

Man kann eine Formel ϕ in der klassischen Logik auch durch einen Widerspruchsbeweis herleiten³. Man nimmt das Gegenteil von ϕ an und führt diese Annahme zum Widerspruch. Die Regel sagt dann, dass nach diesem Widerspruchsbeweis ϕ bewiesen ist.

Dass aus dem Widerspruch jede beliebige Aussage folgt, wird auch als *Ex falso quodlibet* oder genauer *Ex falso sequitur quodlibet* bezeichnet.

5.2 Beispiele für das natürliche Schließen

5.2.1 Gentzens Beispiel

Als erstes Beispiel nehmen wir ein Beispiel aus der Arbeit von Gerhard Gentzen, mit der er das natürliche Schließen motiviert [Gen35].

Bewiesen werden soll die Formel

$$(X \vee (Y \wedge Z)) \rightarrow ((X \vee Y) \wedge (X \vee Z))$$

³In der *intuitionistischen* Logik ist diese Schlussregel nicht erlaubt.

Im folgenden Beweis geben die Angaben rechts die jeweils verwendete Regel an und die Zeile (oder Zeilen), auf die sie angewandt wurden.

1.	$(X \vee (Y \wedge Z))$	angenommen
2.	X	angenommen
3.	$(X \vee Y)$	$\vee i_1$ 2
4.	$(X \vee Z)$	$\vee i_1$ 2
5.	$((X \vee Y) \wedge (X \vee Z))$	$\wedge i$ 3, 4
6.	$(Y \wedge Z)$	angenommen
7.	Y	$\wedge e_1$ 6
8.	$(X \vee Y)$	$\vee i_2$ 7
9.	Z	$\wedge e_2$ [6]
10.	$(X \vee Z)$	$\vee i_2$ 9
11.	$((X \vee Y) \wedge (X \vee Z))$	$\wedge i$ 8, 10
12.	$((X \vee Y) \wedge (X \vee Z))$	$\vee e$ 1, 2-5, 6- 11
13.	$(X \vee (Y \wedge Z)) \rightarrow ((X \vee Y) \wedge (X \vee Z))$	$\rightarrow i$ 1-12

5.2.2 Abgeleitete Regeln der Aussagenlogik

Hat man eine Herleitung $P \vdash Q$, dann kann man sie in anderen Herleitungen wie eine Regel verwenden. Zwar führen wir den Beweis im natürlichen Schließen mit bestimmten Symbolen aus, da jedoch der Beweis selbst ganz unabhängig von der Wahl der speziellen Symbole wie etwa P ist, gilt er für *jedes* solche Symbol und kann deshalb selbst wie eine Regel verwendet werden.

Auf dem Merkblatt für die Regeln des natürlichen Schließens <https://esb-dev.github.io/mat/rules.pdf> sind vier solcher abgeleiteter Regeln aufgeführt, die im Folgenden bewiesen werden.

$$\frac{\phi}{\neg\neg\phi} \quad \neg\neg i \qquad \frac{\neg\neg\phi}{\phi} \quad \neg\neg e$$

$$\frac{\phi \rightarrow \psi \quad \neg\psi}{\neg\phi} \quad MT \qquad \frac{}{\phi \vee \neg\phi} \quad TND$$

Beweis für die Einführung der doppelten Negation:

1. P gegeben
2. $\neg P$ angenommen
3. \perp $\neg e$ 2, 1
4. $\neg \neg P$ $\neg i$ 2-3

Beweis für die Elimination der doppelten Negation:

1. $\neg \neg P$ gegeben
2. $\neg P$ angenommen
3. \perp $\neg e$ 1, 2
4. P RAA 2-3

Beweis für Modus Tollens

1. $P \rightarrow Q$ gegeben
2. $\neg Q$ gegeben
3. P angenommen
4. Q $\rightarrow e$ 1, 3
5. \perp $\neg e$ 2, 4
6. $\neg P$ $\neg i$ 3-5

Beweis für *Tertium Non Datur*

1. $\neg(P \vee \neg P)$ angenommen
2. P angenommen
3. $P \vee \neg P$ $\vee i_1$ 2
4. \perp $\neg e$ 1, 3
5. $\neg P$ $\neg i$ 2-4
6. $P \vee \neg P$ $\vee i_2$ 5
7. \perp $\neg e$ 1, 6
8. $P \vee \neg P$ RAA 1-7

Die Beweise für diese abgeleiteten Regel haben wir mit *konkreten* Formeln, in diesem Fall Primformeln wie P und Q , durchgeführt. Sie als Regel zu verwenden bedeutet jedoch, dass sie für *jede* beliebige Formel gelten, weshalb ja auch in der Formulierung der Regel die Symbole der Metasprache ϕ und ψ verwendet wurden. Da aber in den Beweisen selbst keinerlei spezifische Eigenschaften von P oder Q verwendet wurden, können wir die Beweise für beliebige Formeln abstrahieren — und somit wie Regeln verwenden.

Dies ist in der Logic WorkBench generell der Fall: ein im natürlichen Schließen geführter Beweis kann gespeichert werden (mit der Funktion `export` und dann in anderen Beweisen verwendet werden (siehe [Wiki zum Natürlichen Schließen in lwb](#)).

5.3 Beweisstrategien

In diesem Abschnitt wird an einem Beispiel erläutert, welche Strategien man beim Entwickeln einer Herleitung im natürlichen Schließen verwenden kann.

Als Beispiel nehmen wir:

$$P \rightarrow (Q \vee R) \vdash Q \vee (\neg P \vee R)$$

Der erste Schritt besteht immer darin, dass man die Voraussetzungen als gegeben hinschreibt und dann eine Lücke lässt, der das zu zeigende Ziel folgt. Die Lücke stellt die Beweisverpflichtung dar.

In unserem Beispiel führt dieser erste Schritt zu:

1. $P \rightarrow (Q \vee R)$ angenommen
2. :
3. $Q \vee (\neg P \vee R)$

Im weiteren Vorgehen untersucht man, welche Regeln man anwenden kann. Dazu gibt es zwei Möglichkeiten:

- Bei den Zeilen oberhalb der Beweisverpflichtung gibt es eine Formel, für deren Haupt-Junktor eine Regel zur *Elimination* anwendbar ist. Dann kann man diese Regel *vorwärts* verwenden und erhält eine neue Zeile oberhalb der Beweisverpflichtung — oder man schließt den Beweis ab.
- Bei den Zeilen unterhalb der Beweisverpflichtung gibt es eine Formel, für deren Haupt-Junktor eine Regel zur *Einführung* angewandt werden kann. Dann kann man diese Regel *rückwärts* anwenden und erhält eine neue Zeile (oder einen Block).

In unserem Beispiel ist der Haupt-Junktor der Voraussetzung die Implikation. Um sie auflösen zu können, haben wir als Regel den Modus Ponens, der allerdings nur angewandt werden kann, wenn nicht nur $P \rightarrow (Q \vee R)$ gegeben ist, sondern auch P .

Betrachten wir also das Ziel. Dort ist der Haupt-Junktor die Disjunktion. Diese können wir einführen, wenn eine der Seiten gegeben ist. Das ist aber auch nicht der Fall.

In dieser Situation muss man zu anderen Waffen greifen. Wir können immer die Regel TND vorwärts und die Regel RAA rückwärts anwenden.

In unserem Beispiel scheint TND eine gute Wahl zu sein.

Dann haben wir folgende Situation:

1. $P \rightarrow (Q \vee R)$ angenommen
2. $P \vee \neg P$ TND
3. :
4. $Q \vee (\neg P \vee R)$

In den folgenden Schritten hilft das Anwenden der Regeln für die Elimination von Junktoren bzw. der Einführung von Junktoren.

Wir verwenden die Regel zur Elimination der Disjunktion:

1. $P \rightarrow (Q \vee R)$ angenommen
2. $P \vee \neg P$ TND
3. P angenommen
4. :
5. $Q \vee (\neg P \vee R)$
6. $\neg P$ angenommen
7. :
8. $Q \vee (\neg P \vee R)$
9. $Q \vee (\neg P \vee R)$ $\vee e$

Es ist jetzt nicht mehr schwierig, die beiden Beweisverpflichtungen zu erfüllen:

1.	$P \rightarrow (Q \vee R)$	angenommen
2.	$P \vee \neg P$	TND
3.	P	angenommen
4.	$Q \vee R$	MP 1, 3
5.	Q	angenommen
6.	$Q \vee (\neg P \vee R)$	$\vee i_1 5$
7.	R	angenommen
8.	$\neg P \vee R$	$\vee i_2 7$
9.	$Q \vee (\neg P \vee R)$	$\vee i_2 8$
10.	$Q \vee (\neg P \vee R)$	$\vee e 4, 5-6, 7-9$
11.	$\neg P$	angenommen
12.	$\neg P \vee R$	$\vee i_1 11$
13.	$Q \vee (\neg P \vee R)$	$\vee i_2 12$
14.	$Q \vee (\neg P \vee R)$	$\vee e 2, 3-10, 11-13$

Man mag versucht sein, die genannten Strategie *schematisch* anzuwenden und einfach auszuprobieren, welche Regel anwendbar ist. Dies kann in einfachen Fällen zu einer Herleitung führen, trägt jedoch wenig zum *Verständnis* des bewiesenen Sachverhalts bei. Deshalb zum Schluß die

Goldene Regel

Man muss sich die Aussage klarmachen, die man beweisen möchte und einen Beweis formulieren, ohne direkt an die Regeln zu denken, sondern eher wie die *Idee* des Beweises aussehen kann. Erst dann setzt man diese Idee in die Anwendung der Regeln um.

Werkzeuge wie die Logic Workbench eignen sich dann dafür zu überprüfen, ob die Umsetzung der Idee in einzelne Schritte korrekt durchgeführt wurde. Man vermeidet damit Flüchtigkeitsfehler.

5.4 Eigenschaften der Herleitbarkeit \vdash

In diesem Abschnitt betrachten wir Eigenschaften, die die Herleitbarkeit \vdash mittels des natürlichen Schließens hat.

Im Folgenden seien stets Γ, Γ' , Δ Mengen von Formeln der Aussagenlogik sowie ϕ und ψ einzelne Formeln der Aussagenlogik.

Lemma 5.1 (Monotonie).

$$\Gamma \vdash \phi \Rightarrow \Gamma \cup \Delta \vdash \phi$$

Beweis. Monotonie ist eine offensichtliche Eigenschaft von Herleitungen: Zu einer gegebenen Herleitung von ϕ aus Γ kann man weitere Voraussetzungen nach Belieben hinzufügen, sie werden ja für die Herleitung gar nicht notwendigerweise benötigt. \square

Lemma 5.2.

- (a) $\phi \in \Gamma \Rightarrow \Gamma \vdash \phi$
- (b) $\Gamma \vdash \phi \text{ und } \Gamma' \vdash \psi \Rightarrow \Gamma \cup \Gamma' \vdash \phi \wedge \psi$
- (c) $\Gamma \vdash \phi \wedge \psi \Rightarrow \Gamma \vdash \phi \text{ und } \Gamma \vdash \psi$
- (d) $\Gamma \cup \{\phi\} \vdash \psi \Rightarrow \Gamma \vdash \phi \rightarrow \psi$
- (e) $\Gamma \vdash \phi \text{ und } \Gamma' \vdash \phi \rightarrow \psi \Rightarrow \Gamma \cup \Gamma' \vdash \psi$
- (f) $\Gamma \vdash \perp \Rightarrow \Gamma \vdash \phi$
- (g) $\Gamma \cup \{\neg\phi\} \vdash \perp \Rightarrow \Gamma \vdash \phi$

Beweis.

- (a) Wenn $\phi \in \Gamma$ gilt, besteht die Herleitung von ϕ trivialerweise aus der Wiederholung von ϕ .
- (b) Wegen Monotonie gilt $\Gamma \vdash \phi \Rightarrow \Gamma \cup \Gamma' \vdash \phi$ sowie $\Gamma' \vdash \psi \Rightarrow \Gamma \cup \Gamma' \vdash \psi$, also wegen der Regel $\wedge i$ auch $\Gamma \cup \Gamma' \vdash \phi \wedge \psi$.
- (c) Wenn man aus der Herleitung von $\phi \wedge \psi$ mit der Regel $\wedge e_1$ bzw. der Regel $\wedge e_2$ die Konjunktion eliminiert, erhält man $\Gamma \vdash \phi$ bzw. $\Gamma \vdash \psi$.
- (d) Die Aussage gilt wegen der Regel $\rightarrow i$.
- (e) Wegen Monotonie gilt unter den gegebenen Voraussetzung $\Gamma \cup \Gamma' \vdash \phi$ sowie $\Gamma \cup \Gamma' \vdash \phi \rightarrow \psi$, also $\Gamma \cup \Gamma' \vdash \psi$ wegen der Regel $\rightarrow e$, dem Modus Ponens.
- (f) Die Aussage gilt wegen der Regel **EFQ**.
- (g) Eine Herleitung für $\Gamma \vdash \phi$ ergibt sich durch die Regel **RAA**, nach deren Anwendung man die gegebene Herleitung einsetzt und den Widerspruch erhält.

\square

Satz 5.1 (Endlichkeitssatz). *Gilt $\Gamma \vdash \phi$, dann gibt es eine endliche Teilmenge $\Gamma' \subseteq \Gamma$, für die $\Gamma' \vdash \phi$ gilt.*

Beweis. Wenn $\phi \in \Gamma$ ist, dann reicht $\Gamma' = \{\phi\}$ für die Herleitung aus. Für die Induktion über die Länge von Herleitungen setzen wir voraus, dass die Aussage nun für alle Herleitungen der Länge $n - 1$ gelte.

Für eine Herleitung der Länge n , betrachten wir die letzte angewandte Regel. Sie braucht nur endlich viele vorausgesetzte Aussagen, also folgt die Behauptung durch natürliche Induktion. \square

Definition 5.1. (Konsistenz) Eine Menge Γ von Formeln der Aussagenlogik ist *konsistent*, wenn $\Gamma \not\vdash \perp$, *inkonsistent* andernfalls.

Lemma 5.3. Folgende Aussagen sind äquivalent:

- (i) Γ ist konsistent
- (ii) Es gibt kein ϕ mit $\Gamma \vdash \phi$ und $\Gamma \vdash \neg\phi$
- (iii) Es gibt mindestens eine Formel ϕ mit $\Gamma \vdash \neg\phi$

Das Lemma lässt sich auch so formulieren:

Folgende Aussagen sind äquivalent:

- (i') Γ ist inkonsistent
- (ii') Es gibt ein ϕ mit $\Gamma \vdash \phi$ und $\Gamma \vdash \neg\phi$
- (iii') Für alle ϕ gilt $\Gamma \vdash \phi$

Beweis.

- (i') \Rightarrow (iii') Sei ϕ eine beliebige Formel, da Γ inkonsistent ist, gilt $\Gamma \vdash \phi$ nach Lemma 5.2 (f).
- (iii') \Rightarrow (ii') Da alle Formeln herleitbar sind, gibt es ein ϕ mit $\Gamma \vdash \phi$ sowie $\Gamma \vdash \neg\phi$.
- (ii') \Rightarrow (i') Es gibt nach Voraussetzung ein ϕ mit $\Gamma \vdash \phi$ und $\Gamma \vdash \neg\phi$, d.h. $\Gamma \vdash \phi \wedge \neg\phi$, also wegen der Regel $\neg e$ auch $\Gamma \vdash \perp$.

\square

Lemma 5.4.

- (i) $\Gamma \vdash \phi \Leftrightarrow \Gamma \cup \{\neg\phi\} \vdash \perp$
- (ii) $\Gamma \vdash \neg\phi \Leftrightarrow \Gamma \cup \{\phi\} \vdash \perp$

Beweis.

- (i) \Rightarrow) Wenn $\Gamma \vdash \phi$ gilt und zusätzlich die Voraussetzung $\neg\phi$, kann man mit der Regel $\neg e$ den Widerspruch herleiten.
 \Leftarrow) siehe Lemma 5.2 (g).

- (ii) \Rightarrow) Wenn $\Gamma \vdash \neg\phi$ gilt und zusätzlich die Voraussetzung ϕ , kann man mit der Regel $\neg e$ den Widerspruch herleiten.
 \Leftarrow) Eine Herleitung für $\Gamma \vdash \neg\phi$ ergibt sich durch die Regel $\neg i$, nach deren Anwendung man die gegebene Herleitung einsetzt und den Widerspruch erhält.

□

Definition 5.2. (Maximal konsistente Formelmenge) Eine Formelmenge Γ ist *maximal konsistent*, wenn sie konsistent ist, aber jede echte Obermenge $\Gamma' \supset \Gamma$ inkonsistent ist.

Maximal konsistente Mengen sind im Prinzip folgende Mengen von Aussagen: Gegeben sei eine Belegung v und $\Gamma = \{\phi \mid \llbracket \phi \rrbracket_v = T\}$, dann ist diese Menge konsistent und sogar maximal konsistent.

Lemma 5.5. Eine maximal konsistente Menge Γ ist abgeschlossen bezüglich Herleitbarkeit, d.h.

$$\Gamma \vdash \phi \Rightarrow \phi \in \Gamma \text{ für alle } \phi.$$

Beweis. Es gelte für eine maximal konsistente Menge Γ und eine Formel $\phi: \Gamma \vdash \phi$. Angenommen $\phi \notin \Gamma$, dann ist $\Gamma \cup \{\phi\}$ inkonsistent, weil Γ maximal konsistent ist. Also gilt nach Lemma 5.4 $\Gamma \vdash \neg\phi$. D.h. es gibt ein ϕ mit $\Gamma \vdash \phi$ und $\Gamma \vdash \neg\phi$, d.h. Γ ist inkonsistent. □

Lemma 5.6. Eine maximal konsistente Menge Γ ist negationstreu, d.h. für eine beliebige Formel ϕ gilt

$$\text{entweder } \Gamma \vdash \phi \text{ oder } \Gamma \vdash \neg\phi.$$

Beweis. Gilt $\Gamma \vdash \phi$, dann kann wegen der Konsistenz von Γ nicht $\Gamma \vdash \neg\phi$ gelten.

Gilt $\Gamma \not\vdash \phi$, dann ist $\Gamma \cup \{\neg\phi\}$ konsistent (Lemma 5.2 (g)). Da Γ maximal konsistent ist, folgt dann $\neg\phi \in \Gamma$, und somit $\Gamma \vdash \neg\phi$. □

5.5 Vollständigkeit des natürlichen Schließens

Mit dem Beweissystem des natürlichen Schließens haben wir eine weiteren Zugang zur Aussagenlogik neben der semantischen Sicht, wie bereits oben erwähnt:

Sei $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$ eine Menge von Formeln und ϕ eine Formel, dann gibt es zwei Sichten auf die Frage, ob ϕ aus Γ folgt:

- *Semantische Sicht*

$$\Gamma \vDash \phi$$

In allen Modellen (allen „möglichen Welten“), in denen $\gamma_1, \gamma_2, \dots, \gamma_n$ gelten, ist auch ϕ wahr.

- *Syntaktische Sicht*

$$\Gamma \vdash \phi$$

Man kann aus den gegebenen Formeln $\gamma_1, \gamma_2, \dots, \gamma_n$ die Formel ϕ herleiten, indem man ausschließlich die Regel des Beweissystems verwendet.

Nun stellt sich natürlich die Frage, ob die beiden Zugänge gleichwertig sind. Im Grunde handelt es sich im zwei Fragen:

- Ist das Beweissystem *korrekt*? Anders gesagt: wir können aus wahren Voraussetzungen nur wahre Schlüsse ziehen.

$$\Gamma \vdash \phi \Rightarrow \Gamma \vDash \phi$$

- Ist das Beweissystem *vollständig*? Ist es möglich mit den Regeln auch jede in der Semantik zutreffende Schlussfolgerung herzuleiten, also die Umkehrung:

$$\Gamma \vDash \phi \Rightarrow \Gamma \vdash \phi$$

Die erste Frage, die nach der *Korrektheit* des natürlichen Schließens, ist die einfache Angelegenheit, schließlich haben wir die Regeln ja so ausgewählt, dass sie Wahrheit erhalten. Die zweite Frage, die nach der *Vollständigkeit* des Beweissystems, ist schwieriger einzusehen, weil ja nicht auf Anhieb erkennbar ist, wie wir aus der semantischen Sicht auf die Existenz einer Herleitung schließen können, oder sie sogar konstruieren können.

Es sei noch bemerkt, dass es neben dem natürlichen Schließen noch andere Beweissysteme für die Aussagenlogik gibt, zum Beispiel das Hilbert-Kalkül, Gentzen's Sequenzenkalkül oder die Resolution. Für alle diese Beweissysteme kann man die Vollständigkeit zeigen. Vollständigkeit ist also eine Eigenschaft der Logik selbst: es gibt die Möglichkeit ein Kalkül zu finden, mit denen durch rein symbolische Manipulation von Formeln jede semantisch wahre Aussage gezeigt werden kann.⁴

⁴“However, completeness should be understood not as a statement about these specific rules, but as a statement about the logic itself. Completeness asserts the existence of a list of rules that allows us to deduce every consequence from any set of formulas of the logic.” [Hed04, S.44]

Zum Begriff *Vollständigkeit* Wir hatten in der Einleitung 1.2 schon den Begriff der Vollständigkeit und auch in 4.4 war von „funktionaler Vollständigkeit“ die Rede. Man muss diese drei Bedeutungen auseinanderhalten⁵:

- Eine Menge von Booleschen Operatoren heißt *funktional vollständig*, wenn man jede Boolesche Funktion $f : \mathbb{B}^n \rightarrow \mathbb{B}, n \geq 1$ durch diese Operatoren darstellen kann, siehe 4.4.
- Eine durch ein Axiomensystem definierte Theorie heißt *vollständig*, wenn jede geschlossene Formel oder ihre Negation in der Theorie enthalten ist, siehe 1.2.
- Ein Beweissystem, Kalkül für eine Logik heißt *vollständig*, wenn jedes richtige Theorem auch mit den Regeln des Kalküls hergeleitet werden kann. Dieser Begriff von Vollständigkeit ist das Thema in diesem Abschnitt. Man sieht leicht, dass damit nicht Vollständigkeit im Sinne einer vollständigen Theorie gemeint ist, denn die Formel P kann in der Aussagenlogik offensichtlich weder als wahr noch als falsch bewiesen werden.

5.5.1 Korrektheit des natürlichen Schließens für die Aussagenlogik

Satz 5.2 (Korrektheit des natürlichen Schließens).

$$\Gamma \vdash \phi \Rightarrow \Gamma \vDash \phi$$

(Informeller) Beweis:

Zunächst muss man präzise sagen, was in Herleitungen erlaubt ist.

Dazu muss man unterscheiden zwischen Regeln, die man einfach dadurch anwenden kann, indem man syntaktisch die Ausdrücke über dem Strich der Regel durch den Ausdruck unter dem Strich ersetzt. Ein Beispiel ist die Einführung von \wedge aus zwei gegebenen Formeln.

Andere Regeln sind so aufgebaut, dass sie selbst wieder eine Beweisverpflichtung enthalten, wie etwa die Einführung von $\phi \rightarrow \psi$. Für diesen Schritt wird angenommen, dass ϕ bereits hergeleitet wurde und man zeigt unter dieser Annahme, dass man dann ψ herleiten kann. In diesem Fall darf die Annahme ϕ nicht außerhalb des Bereichs der Beweisverpflichtung verwendet werden.

⁵Der Wikipedia-Artikel über [Vollständigkeit in der Logik](#) beschreibt die drei Bedeutungen des Begriffs recht gut.

Um es mit Richard Bornat auszudrücken [Bor05, Definition 5.2, Seite 56] auszudrücken:

In a box-and-line proof

1. every line must be justified either as a premise or by use of a rule appealing to *previous* lines or boxes;
2. if an appealed-to line is inside a box, then that box must also enclose the justified line.

Wenn eine Herleitung diese Bedingungen erfüllt, dann wird sie wahre Aussagen in wahre Aussagen überführen, wenn jede der Regeln des natürlichen Schließens das tun. Man muss also für jede Regel überprüfen, ob sie Wahrheit erhält.

Zwei Beispiele für die Argumentation, die Korrektheit der restlichen Regeln kann man ähnlich überprüfen:

Die Regel $\frac{\phi \quad \psi}{\phi \wedge \psi}$ erhält Wahrheit, denn sind die Voraussetzungen wahr, dann auch die Folgerung. Das ist gerade die semantische Definition von \wedge .

$$\boxed{\begin{array}{c} \phi \\ \vdots \\ \psi \end{array}}$$

Die Regel $\frac{\phi}{\phi \rightarrow \psi}$ Wenn wir annehmen, dass $\llbracket \phi \rrbracket = T$ und es gelingt unter Anwendung unserer wahrheitserhaltender Regeln zu zeigen, dass dann auch ψ wahr ist, dann bedeutet das, dass $\llbracket \phi \rightarrow \psi \rrbracket = T$ ist, wie man an der Wahrheitstafel von \rightarrow sieht. \square

5.5.2 Vollständigkeit des natürlichen Schließens für die Aussagenlogik

Es geht darum, dass jede wahre Aussage auch hergeleitet werden kann. Wir haben also alle Regeln, die dafür erforderlich sind. Ordentlicher ausgedrückt:

Satz 5.3 (Vollständigkeit des natürlichen Schließens).

$$\Gamma \vDash \phi \Rightarrow \Gamma \vdash \phi$$

Man kann diesen Satz durch einen Widerspruchsbeweis zeigen. In Büchern über mathematische Logik wird gerne diese Art des Beweises verwandt.

Eine andere Möglichkeit des Beweises besteht darin, dass man aus der gegebenen wahren Aussage eine Herleitung des natürlichen Schließens *konstruiert*. Man zeigt also, dass man ein Programm schreiben kann, das die Herleitung ausgibt und wie es dies tun müsste. Dies ist eine Art des Beweises, die einem Informatiker naheliegt, so wird der Beweis etwa in [HR04] geführt.

Wir wollen beide Beweise kennenlernen, in diesem Abschnitt zunächst den indirekten Beweis.

Wir benötigen zwei wichtige Sätze, um den Widerspruchsbeweis führen zu können:

Satz 5.4 (Satz von Lindenbaum). *Jede konsistente Menge Γ kann zu einer maximal konsistenten Menge $\Gamma^* \supseteq \Gamma$ erweitert werden.*

Beweis. Wir setzen für den Beweis voraus, dass unsere Sprache abzählbar viele Formeln enthält⁶: $\phi_0, \phi_1, \phi_2, \dots$. Nun kann man eine aufsteigende Folge von Formelmengen definieren, deren Vereinigung maximal konsistent ist.

Die Konstruktion geht so:

$$\begin{aligned}\Gamma_0 &= \Gamma \\ \Gamma_{n+1} &= \begin{cases} \Gamma_n \cup \{\phi_n\} & \text{falls } \Gamma_n \cup \{\phi_n\} \text{ konsistent} \\ \Gamma_n & \text{sonst} \end{cases} \\ \Gamma^* &= \bigcup \{\Gamma_n \mid n \geq 0\}\end{aligned}$$

Es ist nun zu zeigen, dass Γ^* konsistent und maximal konsistent ist:

Jede der Formelmengen Γ_n ist konsistent, so wurden sie ja konstruiert.

Nehmen wir nun an, ihre Vereinigung Γ^* wäre nicht konsistent. Dann könnte man aus Γ^* den Widerspruch herleiten. Für diese Herleitung genügen endlich viele der Aussagen aus Γ^* , d.h. aber, dass es ein n gibt, so dass alle die für die Herleitung benötigten Aussagen in Γ_n sind, also $\Gamma_n \vdash \perp$, aber Γ_n ist konsistent. Die Annahme ist also widerlegt, Γ^* ist konsistent.

Es bleibt zu zeigen, dass Γ^* maximal konsistent ist. Nehmen wir eine konsistente Menge von Aussagen $\Delta \supseteq \Gamma^*$. Ist $\phi \in \Delta$, dann ist ϕ eine der Formeln ϕ_i , und demzufolge in Γ_{i+1} enthalten, also in Γ^* , d.h. $\Delta = \Gamma^*$. \square

⁶Man kann den Beweis auch für überabzählbare Mengen führen, siehe [Rau08, Lemma 4.3]

Satz 5.5 (Modellexistenzsatz). *Eine konsistente Menge Γ ist erfüllbar.*

Beweis. Wir können wegen dem Satz von Lindenbaum annehmen, dass Γ eine maximale konsistente Menge ist. Wir definieren eine Belegung, indem wir auf den Primformeln festlegen

$$v(P_i) = \begin{cases} T & \text{für } P_i \in \Gamma \\ F & \text{sonst} \end{cases}$$

Nun muss man also zeigen, dass für eine beliebige Formel ϕ gilt:

$$v(\phi) = T \Leftrightarrow \phi \in \Gamma$$

Dazu kann man strukturelle Induktion über den Aufbau der Formeln machen. Da wir wissen, dass die Junktoren \wedge und \neg funktional vollständig ist, genügt es die Induktion für diese beiden Junktoren zu machen.

1. Für Primformeln gilt die Behauptung per Definition der Belegung.

2. Für $\phi = \psi \wedge \chi$:

$v(\phi) = T \Leftrightarrow v(\psi) = v(\chi) = T$ also durch die Induktionsvoraussetzung: $\psi, \chi \in \Gamma$, also auch $\phi \in \Gamma$ wegen der Maximalität von Γ .

Umgekehrt: Maximale konsistente Mengen sind abgeschlossen bezüglich Herleitbarkeit (Lemma 5.5), d.h. $\psi \wedge \chi \in \Gamma \Leftrightarrow \psi, \chi \in \Gamma$, also $v(\phi) = T$.

3. Für $\phi = \neg\psi$:

$v(\phi) = T \Leftrightarrow v(\psi) = F$ also durch die Induktionsvoraussetzung: $\psi \notin \Gamma$ und $\phi \in \Gamma$.

Umgekehrt: $\phi \in \Gamma$ ergibt $\psi \notin \Gamma$, also $v(\psi) = F$, also $v(\phi) = T$.

Aus der strukturellen Induktion folgt die Aussage, wir haben ein Modell konstruiert. \square

Nun können wir den Vollständigkeitssatz beweisen:

Beweis des Vollständigkeitssatzes. Zu zeigen ist, dass $\Gamma \models \phi \Rightarrow \Gamma \vdash \phi$ gilt. Wir nehmen das Gegenteil an, dass also zwar $\Gamma \models \phi$, aber $\Gamma \not\vdash \phi$ der Fall ist.

Wenn $\Gamma \not\vdash \phi$, dann ist $\Gamma \cup \{\neg\phi\}$ konsistent. Nach dem Satz von Lindenbaum gibt es eine maximale konsistente Erweiterung Γ^* für $\Gamma \cup \{\neg\phi\}$. Nach dem Modellexistenzsatz gibt es ein Modell für Γ^* , das alle diese Formeln wahr macht. Also ist dann auch $\neg\phi$ wahr, das bedeutet aber, dass $\Gamma \not\models \phi$ gelten würde, was der Voraussetzung widerspricht. \square

5.5.3 Ein konstruktiver Beweis für den Vollständigkeitssatz in der Aussagenlogik

Für den konstruktiven Beweis setzen wir voraus, dass die Menge Γ endlich ist und es gilt $\Gamma \vDash \phi$. Es ist dann zu zeigen, dass $\Gamma \vdash \phi$ gilt, indem wir angeben, wie man eine Herleitung erstellen kann.

Zunächst reduzieren wir die Fragestellung auf den Fall einer allgemeingültigen Formel, d.h. auf

$$\vDash \phi \Rightarrow \vdash \phi$$

Mit Lemma 5.7 wird aus dem allgemeinen Fall $\Gamma \vDash \phi$ eine allgemeingültige Formel. Wenn wir für diese zeigen, dass es eine Herleitung gibt, können wir mit Lemma 5.8 eine Herleitung $\Gamma \vdash \phi$ finden.

Lemma 5.7. Für Aussagen $\gamma_1, \gamma_2, \dots, \gamma_n$ und ϕ gilt:

$$\gamma_1, \gamma_2, \dots, \gamma_n \vDash \phi \Rightarrow \vDash (\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi)$$

Beweis. Wir betrachten den Syntaxbaum der Formel $\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi$ in Abb. 5.1.

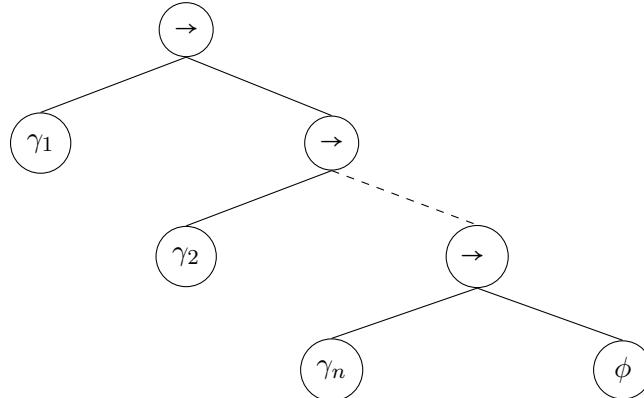


Abbildung 5.1: Syntaxbaum für Lemma 5.7

Angenommen $\not\vDash (\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi)$, d.h. es gibt eine Belegung bei der die Aussage F ergibt. Dann muss die Wurzel des Baums F sein. Das ist nur möglich, wenn $\gamma_1 T$ ist und die zweite Implikation F — und so weiter. Also ergibt sich, dass alle der γ s T sind, aber ϕF . Das steht aber im Widerspruch zur Voraussetzung $\gamma_1, \gamma_2, \dots, \gamma_n \vDash \phi$. \square

Lemma 5.8. Für Aussagen $\gamma_1, \gamma_2, \dots, \gamma_n$ und ϕ gilt:

$$\vdash (\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi) \Rightarrow \gamma_1, \gamma_2, \dots, \gamma_n \vdash \phi$$

Beweis. Nach Voraussetzung gibt es eine Herleitung für $\vdash (\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \gamma_n \rightarrow \phi)$. Wir müssen einen Beweis konstruieren für $\gamma_1, \gamma_2, \dots \gamma_n \vdash \phi$.

Wir gehen so vor:

1.	γ_1	gegeben
2.	γ_2	gegeben
:	:	:
n.	γ_n	gegeben
:	$\vdash \quad \vdots$	Beweis aus der Voraussetzung
m.	$\gamma_1 \rightarrow \gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi$	
m+1.	$\gamma_2 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi$	$\rightarrow e 1, m$
m+2.	$\gamma_3 \rightarrow \dots \rightarrow \gamma_n \rightarrow \phi$	$\rightarrow e 2, m+1$
:	:	:
m+n.	ϕ	$\rightarrow e n, m+n-1$

□

Mit diesen beiden Lemmas haben wir Aufgabe darauf reduziert, zu zeigen, dass

$$\vDash \phi \Rightarrow \vdash \phi$$

gilt. Die Idee des Beweise besteht darin, aus der Wahrheitstafel der Formel ϕ die Herleitung zu konstruieren.

Lemma 5.9. ϕ sei eine Formel und $\hat{P}_1, \hat{P}_2, \dots, \hat{P}_n$ die Literale der Wahrheitstafel für ϕ . Dann gilt:

1. Wenn der Wert der Zeile T ist, dann gibt es eine Herleitung $\hat{P}_1, \hat{P}_2, \dots, \hat{P}_n \vdash \phi$
2. Wenn der Wert der Zeile F ist, dann gibt es eine Herleitung $\hat{P}_1, \hat{P}_2, \dots, \hat{P}_n \vdash \neg\phi$

Beweis. Der Beweis geht durch strukturelle Induktion über den Formelaufbau:

Wenn die Formel atomar ist, etwa P , dann muss man zeigen, dass $P \vdash P$ und $\neg P \vdash \neg P$. Diese Beweise sind einfach die Übernahme der gegebenen Aussage in die Schlussfolgerung.

Wenn die Formel nicht atomar ist, dann hat sie eine (bei \neg als Hauptjunktor) oder zwei Subformeln. Nach Induktionsvoraussetzung können wir voraussetzen, dass das Lemma für diese Subformeln bereits gilt. Das

bedeutet, dass wir für jeden Junktor einen Beweis für alle Fälle seiner zugeordneten Wahrheitstafel finden müssen.

Falls $\phi = \neg\phi_1$:

Wenn $\phi \equiv T$ ist, brauchen wir einen Beweis $\neg\phi_1 \vdash \neg\phi_1$, was automatisch gilt.

Wenn $\phi \equiv F$ ist, brauchen wir einen Beweis $\phi_1 \vdash \neg\neg\phi_1$:

1. ϕ_1 gegeben
2. $\neg\phi_1$ angenommen
3. \perp $\neg e$ 2, 1
4. $\neg\neg\phi_1$ $\neg i$ 2-3

Falls $\phi = \phi_1 \rightarrow \phi_2$:

Wenn $\phi \equiv T$ müssen wir drei Fälle betrachten, nämlich ϕ_1 ist F oder ϕ_2 ist T:

1. $\neg\phi_1$ gegeben
2. ϕ_2 gegeben
3. ϕ_1 angenommen
4. ϕ_2 übernommen 2
5. $\phi_1 \rightarrow \phi_2)$ $\rightarrow i$ 3-4

1. $\neg\phi_1$ gegeben
2. $\neg\phi_2$ gegeben
3. ϕ_1 angenommen
4. \perp $\neg e$ 1, 3
5. ϕ_2 EFQ 4
6. $\phi_1 \rightarrow \phi_2$ $\rightarrow i$ 3-5

1. ϕ_1 gegeben
2. ϕ_2 gegeben
3. ϕ_1 angenommen
4. ϕ_2 übernommen 2
5. $\phi_1 \rightarrow \phi_2$ $\rightarrow i$ 3-4

Bleibt für die Implikation noch der Fall, dass ϕ zu F auswertet:

1. ϕ_1 gegeben
2. $\neg\phi_2$ gegeben
3. $\boxed{\phi_1 \rightarrow \phi_2 \text{ angenommen}}$
4. $\phi_2 \rightarrow e 3, 1$
5. $\perp \neg e 2, 4$
6. $\neg(\phi_1 \rightarrow \phi_2) \neg i 3-5$

Falls $\phi = \phi_1 \wedge \phi_2$:

Wenn ϕ zu T auswertet, haben wir einen Fall zu betrachten:

1. ϕ_1 gegeben
2. ϕ_2 gegeben
3. $\phi_1 \wedge \phi_2 \wedge i 1, 2$

Ist $\phi \equiv F$ sind drei Fälle zu zeigen:

1. ϕ_1 gegeben
2. $\neg\phi_2$ gegeben
3. $\boxed{\phi_1 \wedge \phi_2 \text{ angenommen}}$
4. $\phi_2 \wedge e_2 3$
5. $\perp \neg e 2, 4$
6. $\neg(\phi_1 \wedge \phi_2) \neg i 3-5$

Der Fall $\neg\phi_1$ und ϕ_2 ist symmetrisch zum eben gezeigten Fall.

Für den Fall $\neg\phi_1$ und $\neg\phi_2$ kann man obigen Beweis verwenden, denn die Aussage in Zeile 1 haben wir für die Herleitung ja garnicht verwendet, sie funktioniert also auch, wenn statt ϕ_1 ϕ_1 gegeben ist.

Falls $\phi = \phi_1 \vee \phi_2$:

Ist $\phi \equiv T$ haben wir drei Fälle zu betrachten:

1. ϕ_1 gegeben
2. ϕ_2 gegeben
3. $\phi_1 \vee \phi_2 \vee i_1 1$

Diese Herleitung geht auch, wenn $\neg\phi_2$ vorausgesetzt wird. Und nehmen wir den Fall, dass $\neg\phi_1$ gilt, gibt es die symmetrische Herleitung mit der Regel $\vee i_2$.

Ist schließlich $\phi \equiv F$ können wir folgende Herleitung nehmen:

1.	$\neg\phi_1$	gegeben
2.	$\neg\phi_2$	gegeben
3.	$\phi_1 \vee \phi_2$	angenommen
4.	ϕ_1	angenommen
5.	\perp	$\neg e 1, 4$
6.	ϕ_2	angenommen
7.	\perp	$\neg e 2, 6$
8.	\perp	$\vee e 3, 4-5], 6-7$
9.	$\neg(\phi_1 \vee \phi_2)$	$\neg i 3-8$

□

Nun können wir den konstruktiven Beweis des Vollständigkeitssatzes abschließen, in dem wir zeigen, dass

$$\vDash \phi \Rightarrow \vdash \phi$$

gilt.

Beweis. Da $\vDash \phi$ gilt, hat die Formel ϕ eine Wahrheitstafel, in der alle Zeilen zu T auswerten. Seien P_1, P_2, \dots, P_n die Aussagensymbole in ϕ . Die Wahrheitstafel hat dann 2^n Zeilen.

Wir beginnen die Konstruktion der Herleitung, indem wir mit der Regel TND als erste Zeile der Herleitung $P_1 \vee P_2$ einführen. Der nächste Schritt besteht dann darin, dass wir zwei Unterbeweise für die Auflösung des \vee der ersten Zeile aufmachen. In jeder dieser beiden Boxen wenden wir nun erneut die Regel TND mit P_2 , gefolgt von $\vee e$.

Nach zwei Schritten sieht die Herleitung so aus:

1.	$P_1 \vee \neg P_1$	TND
2.	P_1	angenommen
3.	$P_2 \vee \neg P_2$	TND
4.	P_2	angenommen
5.	:	
6.	ϕ	
7.	$\neg P_2$	angenommen
8.	:	
9.	ϕ	
10.	ϕ	ve
11.	$\neg P_1$	angenommen
12.	$P_2 \vee \neg P_2$	TND
13.	P_2	angenommen
14.	:	
15.	ϕ	
16.	$\neg P_2$	angenommen
17.	:	
18.	ϕ	
19.	ϕ	ve
20.	ϕ	ve

Wenn man das Verfahren abwechselnd die Regel TND und die Auflösung von \vee bis zu P_n fortsetzt, dann hat man 2^n Boxen mit Beweisverpflichtungen. Jede der Boxen entspricht genau einer Zeile der Wahrheitstafel und hat als Voraussetzungen die entsprechenden Literale \hat{P}_i .

In jeder Box können wir nach Lemma 5.9 eine Herleitung rekursiv konstruieren. Diese Herleitungen fügen wir an Stelle der Beweisverpflichtungen ein — und so erhalten wir eine Herleitung für ϕ . \square

Bemerkung In Lemma 5.9 und im Beweis eben wurden alle Regeln zur Einführung und Auflösung von $\wedge, \vee, \rightarrow, \neg$ verwendet, außerdem EFQ und TND. Dies zeigt, dass diese Regeln für das natürliche Schließen in der klassischen Aussagenlogik ausreichend sind.

5.5.4 Kompaktheitssatz

Der Vollständigkeitssatz hat eine wichtige Folgerung, den Endlichkeitsatz der Erfüllbarkeit oder den *Kompaktheitssatz*:

Satz 5.6 (Kompaktheitssatz). *Eine Menge Γ von Aussagen ist erfüllbar, wenn jede endliche Teilmenge von Γ erfüllbar ist.*

Beweis. Wir zeigen die Kontraposition: Wenn Γ nicht erfüllbar ist, dann gibt es eine endliche Teilmenge von Γ , die nicht erfüllbar ist.

Nehmen wir also an, dass Γ nicht erfüllbar ist. Nach dem Vollständigkeitssatz gilt dann $\Gamma \vdash \perp$. Ein solcher Beweis kommt aber mit einer endlichen Menge von Voraussetzungen Γ' aus. Das bedeutet, dass es eine endliche Teilmenge von Γ gibt, eben Γ' , die nicht erfüllbar ist. \square

Kapitel 6

Normalformen

6.1 Negationsnormalform NNF

Wir beobachten zunächst, dass man jede Formel äquivalent so umformen kann, dass sie keine Implikationen mehr enthält. Dazu verwendet man die Äquivalenz $\phi \rightarrow \psi \equiv \neg\phi \vee \psi$.

Definition 6.1 (Literal). Ein *Literal* ist eine Primaussage P oder ihre Negation $\neg P$.

Wir formulieren einen Algorithmus für die Elimination der Implikation aus aussagenlogischen Formeln:

```
function IMPL_FREE( $\phi$ ) {
    // pre: beliebige Formel  $\phi$ 
    // post: äquivalente Umformung von  $\phi$ , die kein  $\rightarrow$  mehr enthält
    case {
         $\phi$  ist Literal:
            return  $\phi$ ;
         $\phi$  hat die Form  $\neg\phi_1$ :
            return  $\neg\text{IMPL\_FREE}(\phi_1)$ ;
         $\phi$  hat die Form  $\phi_1 \wedge \phi_2$ :
            return  $\text{IMPL\_FREE}(\phi_1) \wedge \text{IMPL\_FREE}(\phi_2)$ ;
         $\phi$  hat die Form  $\phi_1 \vee \phi_2$ :
            return  $\text{IMPL\_FREE}(\phi_1) \vee \text{IMPL\_FREE}(\phi_2)$ ;
         $\phi$  hat die Form  $\phi_1 \rightarrow \phi_2$ :
            return  $\neg\text{IMPL\_FREE}(\phi_1) \vee \text{IMPL\_FREE}(\phi_2)$ ;
    }
}
```

Definition 6.2 (Negationsnormalform NNF). Eine Formel ϕ ohne Implikation ist in der *Negationsnormalform NNF*, wenn jede Negation direkt vor einer Primaussage steht.

Beispiele

$\neg\neg P$	nicht NNF	$\neg P$	NNF
$\neg(P \wedge Q)$	nicht NNF	$\neg P \vee \neg Q$	NNF
$\neg(P \vee Q)$	nicht NNF	$\neg P \wedge \neg Q$	NNF

Wir formulieren einen Algorithmus, der eine Formel in die Negationsnormalform bringt:

```
function NNF( $\phi$ ) {
    // pre:  $\phi$  hat keine Implikationen
    // post: äquivalente Umformung von  $\phi$  in NNF
    case {
         $\phi$  ist Literal:
            return  $\phi$ ;
         $\phi$  hat die Form  $\neg\neg\phi_1$ :
            return NNF( $\phi_1$ );
         $\phi$  hat die Form  $\phi_1 \wedge \phi_2$ :
            return NNF( $\phi_1$ )  $\wedge$  NNF( $\phi_2$ );
         $\phi$  hat die Form  $\phi_1 \vee \phi_2$ :
            return NNF( $\phi_1$ )  $\vee$  NNF( $\phi_2$ );
         $\phi$  hat die Form  $\neg(\phi_1 \wedge \phi_2)$ :
            return NNF( $\neg\phi_1 \vee \neg\phi_2$ );
         $\phi$  hat die Form  $\neg(\phi_1 \vee \phi_2)$ :
            return NNF( $\neg\phi_1 \wedge \neg\phi_2$ );
    }
}
```

6.2 Konjunktive Normalform CNF

Definition 6.3 (Klausel). Eine Formel der Form $\phi = \hat{P}_1 \vee \hat{P}_2 \vee \dots \vee \hat{P}_n$ mit Literalen \hat{P}_i nennt man eine *Klausel*.

Beispiele:

$P \vee \neg Q \vee \neg R$ ist eine Klausel
 $\neg P_1 \vee \neg P_2 \vee \dots \vee \neg P_n \vee Q$ ist eine Klausel,
sie ist äquivalent zu
 $P_1 \wedge P_2 \wedge \dots \wedge P_n \rightarrow Q$.

Bemerkung: Oft stellt man Klauseln als Mengen von Literalen dar, wobei mit \bar{P} die Negation $\neg P$ einer Primaussage bezeichnet wird. Der Grund dafür besteht darin, dass logischen Operationen mit Formeln in konjunktiver Normalform und Klauseln mengentheoretischen Operationen auf Klauselmengen und Klauseln entsprechen.

Beispiele: Korrespondierend zu obigen Beispielen

$$\begin{aligned} &\{P, \bar{Q}, \bar{R}\} \\ &\{\bar{P}_1, \bar{P}_2, \dots, \bar{P}_n, Q\} \end{aligned}$$

Definition 6.4 (Konjunktive Normalform CNF). Eine Formel ϕ ist in der *konjunktiven Normalform CNF*, wenn sie die Form $\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n$ hat mit lauter Klauseln ϕ_i .

Wir formulieren einen Algorithmus, der eine Formel in die konjunktive Normalform bringt:

```
function DISTR( $\phi_1, \phi_2$ ) {
    // pre:  $\phi_1$  und  $\phi_2$  sind in CNF
    // post: berechnet CNF für  $\phi_1 \vee \phi_2$ 
    case {
         $\phi_1$  hat die Form  $\phi_{11} \wedge \phi_{12}$ :
            return DISTR( $\phi_{11}, \phi_2$ )  $\wedge$  DISTR( $\phi_{12}, \phi_2$ );
         $\phi_2$  hat die Form  $\phi_{21} \wedge \phi_{22}$ :
            return DISTR( $\phi_1, \phi_{21}$ )  $\wedge$  DISTR( $\phi_1, \phi_{22}$ );
        default:
            return  $\phi_1 \vee \phi_2$ ;
    }
}
```

Mit Hilfe der Hilfsfunktion DISTR ist es nun einfach, einen Algorithmus für das Erzeugen der CNF zu formulieren:

```
function CNF( $\phi$ ) {
    // pre:  $\phi$  ist in NNF
    // post: eine zu  $\phi$  äquivalente Formel in CNF
    case {
         $\phi$  ist Literal:
            return  $\phi$ ;
         $\phi$  hat die Form  $\phi_1 \wedge \phi_2$ :
            return CNF( $\phi_1$ )  $\wedge$  CNF( $\phi_2$ );
         $\phi$  hat die Form  $\phi_1 \vee \phi_2$ :
            return DISTR(CNF( $\phi_1$ ), CNF( $\phi_2$ ));
    }
}
```

}

}

6.3 Disjunktive Normalform DNF

Definition 6.5 (Monom). Eine Formel der Form $\psi = \hat{P}_1 \wedge \hat{P}_2 \wedge \dots \wedge \hat{P}_n$ mit Literalen \hat{P}_i bezeichnet man als *Monom*.

Definition 6.6 (Disjunktive Normalform DNF). Eine Formel ψ ist in der *disjunktiven Normalform DNF*, wenn sie die Form $\psi_1 \vee \psi_2 \vee \dots \vee \psi_n$ hat mit lauter Monomen ψ_i .

Beobachtung: („Dualität“ von CNF und DNF)

Ist die Formel ϕ in CNF, dann ist $\neg\phi$ modulo simpler Transformationen in DNF.

Ist ϕ in CNF, dann hat ϕ die Form $\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n$ mit Klauseln ϕ_i .

Betrachte nun $\neg\phi$, also $\neg(\phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_n)$.

Nach De Morgan ist dies äquivalent zu $\neg\phi_1 \vee \neg\phi_2 \vee \dots \vee \neg\phi_n$.

Wendet man nun De Morgan auch auf die Klauseln ϕ_i an und eliminiert doppelte Negation, dann erhält man Monome und die Formel $\neg\phi$ ist in DNF.

6.4 Normalformen und Entscheidungsprobleme

Ein *komplementäres* Paar von Literalen ist eine Primaussage samt seiner Negation, also z.B. P und $\neg P$.

6.4.1 CNF und Gültigkeit

Satz 6.1 (CNF und Gültigkeit). *Sei ϕ in CNF. Dann gilt:*

ϕ ist allgemeingültig \Leftrightarrow Jede Klausel enthält ein komplementäres Paar von Literalen

Beweis. Wenn ϕ allgemeingültig ist, dann könnte man sich als kürzeste Darstellung in CNF \top vorstellen, \top gehört aber nicht zum Alphabet unsere Sprache. Eine Darstellung der Formel in CNF enthält also Klauseln mit Aussagensymbolen aus ϕ . Diese Klauseln sind mit \wedge verbunden, müssen also alle zu \top auswerten, damit die Formel wahr wird. Eine Klausel kann aber nur zu \top auswerten, wenn sie ein komplementäres Paar von Literalen enthält. \square

6.4.2 DNF und Erfüllbarkeit

Satz 6.2 (DNF und Erfüllbarkeit). *Sei ψ in DNF. Dann gilt:
 ψ ist unerfüllbar \Leftrightarrow Jedes Monom enthält ein komplementäres Paar von Literalen*

Beweis. Die kürzeste Darstellung von ψ ist \perp . Angenommen die Kontradiktion ψ ist als Disjunktion von Monomen dargestellt. Dann müssen diese alle ebenfalls Kontradiktionen sein. Ein Monom ist genau dann unerfüllbar, wenn sie ein komplementäres Paar von Literalen enthält. \square

Übung. Vorausgesetzt ϕ ist eine Tautologie in konjunktiver Normalform CNF, wie kann man dann daraus eine Herleitung von ϕ nach den Regeln des natürlichen Schließens *konstruieren*? Diese Übung ergibt einen anderen Beweis der Vollständigkeit des natürlichen Schließens (siehe 5.5).

Kapitel 7

Die Komplexität des Erfüllbarkeitsproblems

7.1 Das Erfüllbarkeitsproblem

7.1.1 Entscheidungsfragen der Aussagenlogik

In der Aussagenlogik kann man sich zu einer gegebenen Formel ϕ folgende Fragen stellen:

- Ist ϕ *allgemeingültig*?

Diese Frage nennt man auch das Gültigkeitsproblem. Die Formel ϕ ist allgemeingültig, wenn sie für jede beliebige Belegung der Aussagensymbole wahr ist. Ist eine Formel ϕ allgemeingültig, nennt man ϕ auch eine *Tautologie*.

- Ist ϕ *unerfüllbar*?

Diese Frage nennt man auch das Unerfüllbarkeitsproblem. Die Formel ϕ ist unerfüllbar, wenn es keine Belegung der Aussagensymbole gibt, die sie wahr macht. Ist eine Formel ϕ unerfüllbar, sagt man auch ϕ ist der *Widerspruch* oder eine *Kontradiktion*.

- Ist ϕ *erfüllbar*?

Diese Frage nennt man auch das Erfüllbarkeitsproblem. Die Formel ϕ ist erfüllbar, wenn es eine Belegung gibt, unter der die Formel wahr ist. In der Regel ist man dann natürlich auch interessiert daran, ein solches Modell zu finden.

- Ist ϕ *falsifizierbar*?

Diese Frage nennt man auch das Widerlegungsproblem. Die Formel ϕ ist falsifizierbar oder widerlegbar, wenn es eine Belegung gibt, unter der die Formel falsch ist. Auch dann möchte man üblicherweise wissen, für welches Modell die Formel falsch ist.

Diese Fragen hängen miteinander zusammen. Denn aus den Definitionen ergibt sich unmittelbar:

- Eine Formel ϕ ist genau dann allgemeingültig, wenn $\neg\phi$ unerfüllbar ist.
- Eine Formel ϕ ist genau dann falsifizierbar, wenn $\neg\phi$ erfüllbar ist.

Also genügt es, die Frage zu betrachten, ob eine Formel *erfüllbar* ist. Wenn ja, unter welcher Belegung?

7.1.2 Das Erfüllbarkeitsproblem

Die Frage, ob eine Formel erfüllbar ist, wird als das *Erfüllbarkeitsproblem*, auch *SAT-Problem* (*SAT* = *satisfiability*) oder ganz kurz *SAT*, bezeichnet.

Es ist nicht schwierig, das Erfüllbarkeitsproblem zu lösen. Hat man eine Formel ϕ , dann stellt man die Wahrheitstafel für die Formel auf und sieht nach, ob es eine Zeile der Wahrheitstafel gibt, in der die Formel wahr ist.

Dieses Vorgehen ist jedoch nur für Formeln mit wenig Atomen geeignet. Hat ϕ n Atome, dann hat die Wahrheitstafel 2^n Zeilen. Hat also zum Beispiel eine Formel 100 Atome und die Untersuchung einer Zeile der Wahrheitstafel dauert 10^{-10} Sekunden, dann dauert die Untersuchung der gesamten Wahrheitstafel $2^{100} \times 10^{-10}$ Sekunden, also etwa 4×10^{12} Jahre. „Das ist länger als die Zeit, die seit der Entstehung des Universums vergangen ist.“¹

7.2 Komplexität von Algorithmen

Ein *Algorithmus* ist ein Verfahren, das in endlich vielen Schritten zur Lösung eines Problems führt. Mit dieser informellen Definition eines Algorithmus wollen wir im Folgenden arbeiten.²

Die *Komplexität* eines Algorithmus wird gemessen durch die Menge an Ressourcen (Zeit oder Speicher), die für die Durchführung des Algorithmus im Prinzip benötigt wird. Wir werden die Laufzeit eines Algorithmus im Folgenden als seine Komplexität betrachten.

¹Die beispielhafte Berechnung der Ineffizienz der Entscheidung des Erfüllbarkeitsproblems durch die Wahrheitstafel ist aus: Uwe Schöning: *Das SAT-Problem* in: Informatik Spektrum Band 33 Heft 5 Oktober 2010

²Präziseres findet man in: Michael Sipser: *Introduction to the Theory of Computation*, Kap. 3.3 The Definition of Algorithm

7.2.1 Arten von Algorithmen

Definition 7.1. Ein Algorithmus ist *deterministisch*, wenn die Berechnung und somit das Ergebnis vollständig durch die Eingabe bestimmt wird. Ein deterministischer Algorithmus ist genau dann *korrekt*, wenn das Ergebnis zur gegebenen Eingabe korrekt ist.

Beispiel 7.1. Der Algorithmus mittels der Wahrheitstafel die Erfüllbarkeit einer Formel zu berechnen ist ein deterministischer Algorithmus für das Erfüllbarkeitsproblem.

Definition 7.2. Ein Algorithmus ist *nichtdeterministisch*, wenn seine Schritte mehrere mögliche Folgeschritte haben, deren Wahl nicht durch die Eingabe und bisherige Berechnung bestimmt wird. Zu einer Eingabe sind also mehrere verschiedene Berechnungsergebnisse möglich. Ein nichtdeterministischer Algorithmus heißt *korrekt*, wenn unter den möglichen Ergebnissen wenigstens eines korrekt ist.

Beispiel 7.2. Ein nichtdeterministischer Algorithmus für das Erfüllbarkeitsproblem ist leicht zu definieren. Der erste Schritt besteht darin, eine Belegung der Aussagensymbole zu raten. Im zweiten Schritt wird die Formel berechnet.

Dieser Algorithmus ist sogar ein korrekter nichtdeterministischer Algorithmus. Wenn die Formel erfüllbar ist, dann gibt es eine erfüllende Belegung. Rät der Algorithmus mal richtig, dann entscheidet er das Erfüllbarkeitsproblem korrekt.

7.2.2 Laufzeit von Algorithmen

Nun definieren wir Maße für die Komplexität von Algorithmen:

Definition 7.3. Ein Algorithmus heißt *polynomiell*, wenn seine Laufzeit nach oben durch ein Polynom in n (n ist die Größe der Eingabe) beschränkt ist. Algorithmen, die in polynomieller Zeit ein korrektes Ergebnis liefern, werden oft auch als *effiziente* Algorithmen bezeichnet.

Beispiel 7.3. Unser nichtdeterministischer Algorithmus durch Erraten das Erfüllbarkeitsproblem zu lösen ist polynomiell: Das Erraten einer Belegung ist linear bezüglich der Größe der Eingabe, d.h. der Anzahl n der Atome und das Überprüfen, ob das Erratene zutrifft ist offensichtlich effizient durchführbar.

Definition 7.4. Ein Algorithmus läuft in *exponentieller* Zeit, wenn die Laufzeit nach unten durch eine Funktion 2^{cn} für die Größe der Eingabe n und ein $c > 0$ beschränkt ist.

Beispiel 7.4. Die Methode mit der Wahrheitstafel die Erfüllbarkeit einer Formel zu entscheiden ist exponentiell: Die Größe der Eingabe ist die Zahl n der Atome der Formel. Im schlechtesten Fall muss man zur Entscheidung alle 2^n Zeilen der Wahrheitstafel konstruieren.

7.2.3 Klassen von Problemen und \mathcal{NP} -Vollständigkeit

Definition 7.5. Die Klasse \mathcal{P} bezeichnet die Probleme, die in polynomieller Zeit durch einen deterministischen Algorithmus gelöst werden können.

Beispiel 7.5. Es ist nicht bekannt, ob das Erfüllbarkeitsproblem zur Klasse \mathcal{P} gehört. Es wird vermutet, dass dies nicht der Fall ist, wie wir gleich genauer diskutieren werden.

Definition 7.6. Die Klasse \mathcal{NP} bezeichnet die Probleme, die ein nicht-deterministischer Algorithmus in polynomieller Zeit lösen kann.

Beispiel 7.6. Das Erfüllbarkeitsproblem gehört zur Klasse \mathcal{NP} . Man sagt auch: SAT ist \mathcal{NP} .

Man kann auch so ausdrücken, dass ein Problem in \mathcal{NP} ist: eine *Lösung* des Problems ist in polynomieller Zeit *überprüfbar*, auch wenn sie möglicherweise nicht in polynomieller Zeit *gefunden* werden kann.

Vermutung: Ist $\mathcal{P} = \mathcal{NP}$? Dies ist eine grundlegende Frage der Informatik, die ungelöst ist.³ Allgemein wird vermutet, dass gilt:

$$\mathcal{P} \neq \mathcal{NP}.$$
⁴

Zur genaueren Bestimmung der Komplexität des Erfüllbarkeitsproblems benötigen wir noch weitere Definitionen:

Definition 7.7. Ein Problem P ist \mathcal{NP} -schwierig, wenn sich jedes Problem Q in \mathcal{NP} deterministisch in polynomieller Zeit auf P reduzieren lässt.

³Das Clay Mathematics Institute <http://www.claymath.org> hat dieses Problem als eines der 7 Millenniums-Probleme ausgewählt – neben u.a. der Riemann-Vermutung oder der (mittlerweile von Grigori Perelman gelösten) Poincaré-Vermutung.

⁴Donald E. Knuth sieht das anders: „... almost everybody who has studied the subject thinks that satisfiability cannot be decided in polynomial time. The author of this book, however, suspects that $N^{O(1)}$ -step algorithms do exist, yet that they're unknowable. Almost all polynomial time algorithms are so complicated that they lie beyond human comprehension, and could never be programmed for an actual computer in the real world. Existence is different from embodiment.“ [Knu15, S. 1]

Definition 7.8. Ein Problem P ist \mathcal{NP} -vollständig, wenn es in \mathcal{NP} und \mathcal{NP} -schwierig ist.

7.3 Die Komplexität des Erfüllbarkeitsproblems

Nun stehen alle Definitionen zur Verfügung, um den Satz zu formulieren, der die Komplexität des Erfüllbarkeitsproblems bestimmt:

Satz 7.1 (Cook 1971, Levin 1973). *Das Erfüllbarkeitsproblem ist \mathcal{NP} -vollständig.⁵*

Wie sieht es mit dem komplementären Problem der Nichterfüllbarkeit bzw. der Allgemeingültigkeit aus? Dieses Problem ist insofern schwieriger, als man ja zeigen muss, dass es kein Modell gibt, bzw. dass die Aussage in allen Belegungen wahr ist. Hier hilft „Raten“ nicht mehr. Genauer sagt man:

Definition 7.9. Ein Problem ist in der Klasse $Co-\mathcal{NP}$, wenn das komplementäre Problem in \mathcal{NP} ist.

Beispiel: Das Nichterfüllbarkeitsproblem ist in $Co-\mathcal{NP}$.

Satz 7.2. $Co-\mathcal{NP} = \mathcal{NP}$ genau dann, wenn Nichterfüllbarkeit in \mathcal{NP} ist.

Vermutung: Es ist nicht bekannt, ob es einen nichtdeterministischen polynomiellen Algorithmus für das Nichterfüllbarkeitsproblem gibt. Man nimmt vielmehr an, dass gilt:

$$Co-\mathcal{NP} \neq \mathcal{NP}$$

Die Ergebnisse über die Komplexität des Erfüllbarkeitsproblems können zu der Annahme verleiten, dass es keinen „effizienten“ Algorithmus für SAT geben kann und deshalb Probleme, die man als aussagenlogische Formeln formulieren kann, nur gelöst werden können, wenn man wenige aussagenlogischen Atome in der Formel hat.

⁵Stephen A. Cook, amerikanischer Informatiker, heute Professor für Informatik in Toronto. Er erhielt 1982 für diesen Satz den Turing-Award. Leonid Levin, ukrainischer Informatiker, hat die Theorie der \mathcal{NP} -Vollständigkeit und den Satz über das Erfüllbarkeitsproblem 1973 entwickelt. Seine Ergebnisse waren im Westen zunächst nicht bekannt. 1978 emigrierte er in die USA.

Dies ist jedoch keineswegs der Fall: „Zum Glück gibt es und gab es Algorithmenentwickler, Theoretiker und Praktiker, die sich von diesem Negativergebnis [Satz von Cook und Levin] nicht abschrecken ließen. Dies hat in den vergangenen Jahren dazu geführt, dass die ‚SAT-Solver‘-Technologie immer weiter vorangeschritten ist [und] dass diese das SAT-Problem lösenden Verfahren heutzutage mit Formeln, die Tausende von Variablen enthalten, in Sekundenbruchteilen fertig werden.“⁶

⁶So schreibt Uwe Schöning im bereits zitierten Artikel. Ein solcher SAT-Solver ist **Sat4j** – siehe <http://www.sat4j.org/>.

Kapitel 8

Hornlogik

Betrachtet man spezielle Klassen von Formeln, dann findet man oft effiziente Algorithmen für die Entscheidung des Erfüllbarkeitsproblems. Eine wichtige solche Klasse sind die Hornformeln¹.

Definition 8.1 (Hornklausel). Eine Klausel $\hat{P}_1 \vee \hat{P}_2 \vee \dots \vee \hat{P}_n$ heißt *Hornklausel*, wenn höchstens eines der Literale \hat{P}_i positiv ist.

Definition 8.2 (Hornformel). Eine Formel ϕ in CNF heißt *Hornformel*, wenn jede Klausel eine Hornklausel ist.

Definition 8.3 (Arten von Hornklauseln).

- Besteht eine Hornklausel nur aus einem positiven Literal, dann heißt sie *Tatsachenklausel*, kurz *Tatsache*.
- Hat eine Hornklausel ein positives Literal und mindestens ein negatives Literal, dann heißt sie *Prozedurklausel* oder *Regel*.
- Hat die Hornklausel kein positives Literal, dann heißt sie *Zielklausel* oder *Frageklausel*, kurz *Ziel*.

Beispiel 8.1 (Hornklauseln und Hornformel).

- $\{P\}$ ist eine Tatsachenklausel,
- $\{\neg P, Q\}$ und $\{\neg P, \neg Q, R\}$ sind Regeln und
- $\{\neg P, \neg R\}$ ist eine Zielklausel.

Die Hornformel in diesem Beispiel ist also:

$$P \wedge (\neg P \vee Q) \wedge (\neg P \vee \neg Q \vee R) \wedge (\neg P \vee \neg R)$$

Wir können Hornformel auch (alternativ) definieren, indem wir eine Grammatik angeben:

¹Alfred Horn, amerikanischer Mathematiker, 1918 - 2001

Definition 8.4 (Hornformel). Eine Hornformel ist eine Formel ϕ der Aussagenlogik, die folgender Grammatik genügt:

$$\begin{aligned} T &:= \top \rightarrow P \text{ für Aussagensymbole } P \text{ (Tatsache)} \\ P &:= P \mid P \wedge P \text{ für Aussagensymbole } P \\ Z &:= P \mid P \rightarrow \perp \text{ (Ziel)} \\ R &:= P \rightarrow Q \text{ für Aussagensymbole } Q \text{ (Regel)} \\ H &:= \phi \wedge T \mid \phi \wedge Z \mid \phi \wedge R \end{aligned}$$

Die Bezeichnungen *Tatsache*, *Regel*, *Ziel* ergeben sich aus folgenden Überlegungen:

1. Jede Hornklausel ist entweder eine Tatsache, eine Regel oder ein Ziel.
2. Eine Tatsache muss wahr sein, d.h. $P \equiv \top \rightarrow P$.
3. Eine Prozedurklausel (Regel) $\neg P_1 \vee \dots \vee \neg P_n \vee Q$ ist äquivalent zu $P_1 \wedge \dots \wedge P_n \rightarrow Q$.
4. Eine Zielklausel $\neg P_1 \vee \dots \vee \neg P_n$ ist äquivalent zu $\neg(P_1 \wedge \dots \wedge P_n)$, also $P_1 \wedge \dots \wedge P_n \rightarrow \perp$.

Beispiel 8.2 (Hornformel). Die Hornformel aus Beispiel 8.1 ausgedrückt mit der Grammatik 8.4:

$$(\top \rightarrow P) \wedge (P \rightarrow Q) \wedge (P \wedge Q \rightarrow R) \wedge (P \wedge R \rightarrow \perp)$$

In der Hornlogik wird typischerweise ein Widerlegungsverfahren verwendet. In der Hornformel wird die angestrebte Aussage als *nicht* wahr angenommen (deshalb ist die Form der Zielklausel so wie oben definiert). Kann man nun die Nichterfüllbarkeit der Hornformel zeigen, sieht man, dass die Zielklausel zutrifft.

Wir formulieren einen Algorithmus für die Entscheidung der Erfüllbarkeit von Hornformeln (den sogenannten Markierungsalgorithmus):

```
function HORN( $\phi$ ) {
    // pre:  $\phi$  ist eine Hornformel
    // post: entscheidet die Frage, ob  $\phi$  erfüllbar ist
    markiere alle  $\top$  in  $\phi$ 
    while ( es gibt  $P_1 \wedge P_2 \wedge \dots \wedge P_n \rightarrow Q$  mit
             $P_1, P_2, \dots, P_n$  markiert, aber  $Q$  nicht) {
        markiere  $Q$ 
```

```

    }
    if (  $\perp$  ist markiert ){
        return „unerfüllbar“
    } else {
        return „erfüllbar“
    }
}

```

Eigenschaften dieses Algorithmus

1. Er entscheidet, ob die Hornformel ϕ erfüllbar ist.
 2. Ist ϕ erfüllbar, dann können wir eine erfüllende Belegung ablesen, nämlich
- $$v(P_i) = \begin{cases} \text{T falls } P_i \text{ markiert ist} \\ \text{F sonst} \end{cases}$$
3. Der Algorithmus endet nach spätestens $n+2$ Markierungsschritten, wenn n die Zahl der Atome in ϕ ist.

Beispiel 8.3 (Markierungsalgorithmus).

Gegeben sei die Aussage P , d.h. $\top \rightarrow P$, eine *Tatsache*.

Ferner sei bekannt, dass folgende *Regeln* gelten: $P \rightarrow Q$ und $P \wedge Q \rightarrow R$. Man möchte nun in dieser Situation wissen, ob $P \wedge R$ gilt.

In der Hornlogik klärt man die Frage durch ein *Widerlegungsverfahren*: Man nimmt an, dass $P \wedge R$ nicht gilt. Durch diese Annahme entsteht folgende Hornformel:

$$(\top \rightarrow P) \wedge (P \rightarrow Q) \wedge (P \wedge Q \rightarrow R) \wedge (P \wedge R \rightarrow \perp)$$

Wenn gezeigt werden kann, dass diese Formel *unerfüllbar* ist, dann hat man gezeigt, dass in der gegebenen Situation $P \wedge R$ gilt. Dies zeigt man nun mit Hilfe des Markierungsalgorithmus:

$$\frac{(\top \rightarrow P) \wedge (P \rightarrow Q) \wedge (P \wedge Q \rightarrow R) \wedge (P \wedge R \rightarrow \perp)}{\begin{array}{cccccccccc} * & & & & & & & & & \\ * & * & * & & * & & & & & * \\ * & * & * & * & * & * & & & & * \\ * & * & * & * & * & * & * & * & * & * \\ * & * & * & * & * & * & * & * & * & * \end{array}}$$

Der Algorithmus endet in diesem Beispiel, wenn \perp markiert ist. Das bedeutet, dass die Formel unerfüllbar ist, d.h. dass in der gegebenen Situation $P \wedge R$ gilt.

Kapitel 9

Erfüllbarkeit und SAT-Solver

Die Entscheidungsfragen der Aussagenlogik lassen sich alle auf das Erfüllbarkeitsproblem zurückspielen.

Ein Programm, das für eine Formel der Aussagenlogik das Erfüllbarkeitsproblem löst (und eine erfüllende Belegung ermittelt), heißt *SAT-Solver*.

Die Kunst in der Entwicklung von SAT-Solvern besteht darin, Algorithmen zu finden, die für große Klassen von Formeln das Problem effizient entscheiden, obgleich es \mathcal{NP} -vollständig ist.¹

Typischerweise setzen SAT-Solver voraus, dass eine Formel in CNF vorliegt. Das Eingabeformat ist üblicherweise DIMACS (vorgeschlagen vom Center for Discrete Mathematics and Theoretical Computer Science <http://dimacs.rutgers.edu/>).

9.1 DIMACS-Format

SAT-Solver verwenden eine einfache Variante des DIMACS-Formats. Eine Formel in CNF wird in einer ASCII-Datei gespeichert, die in drei Sektionen aufgebaut ist:

Zuerst kommen optionale *Kommentarzeilen*, die durch ein kleines c an der ersten Position gekennzeichnet sind.

¹Donald E. Knuth: „The story of satisfiability is the tale of a triumph of software engineering, blended with rich doses of beautiful mathematics. Thanks to elegant new data structures and other techniques, modern SAT solvers are able to deal routinely with practical problems that involve many thousands of variables, although such problems were regarded as hopeless just a few years ago.“[Knu15, S. iv]

Darauf folgt die *Präambel*, die aus einer Zeile der Form

p cnf v c

besteht, wobei v für die Zahl der Atome der Formel² und c für die Zahl der Klauseln steht.

Danach folgen die *Klauseln*. Die Literale werden durch Integers codiert. Dabei steht die positive Zahl für ein Atom, die negative Zahl für seine Negation. Jede Klausel nimmt eine Zeile der Datei ein, sie enthält die Literale getrennt durch Leerzeichen und wird abgeschlossen durch eine 0.

Beispiel ϕ sei die folgende Formel in CNF:

$$\begin{aligned}
 & (P_1 \vee P_2 \vee P_3) \wedge \\
 & (P_1 \vee \neg P_2 \vee \neg P_3) \wedge \\
 & \quad (P_1 \vee \neg P_5) \wedge \\
 & (\neg P_2 \vee \neg P_3 \vee \neg P_5) \wedge \\
 & (\neg P_1 \vee \neg P_2 \vee P_3) \wedge \\
 & \quad (P_4 \vee P_6) \wedge \\
 & \quad (P_4 \vee \neg P_6) \wedge \\
 & \quad (P_2 \vee \neg P_4) \wedge \\
 & \quad (\neg P_3 \vee \neg P_4)
 \end{aligned}$$

Sie wird im DIMACS-Format so geschrieben:

```

c Beispiel DIMACS Vorlesung LfM
p cnf 6 9
1 2 3 0
1 -2 -3 0
1 -5 0
-2 -3 -5 0
-1 -2 3 0
4 6 0
4 -6 0
2 -4 0
-3 -4 0

```

Doch stop! Wir haben gesehen, dass die Umformung einer beliebigen Formel in eine äquivalente Formel in CNF im schlechtesten Fall eine exponentielle Laufzeit (in Bezug auf die Zahl der Atome der Formel) haben kann. Führt das nicht schon von vorneherein dazu, dass die Entscheidung der Erfüllbarkeit *nicht* effizient sein kann, noch ehe der SAT-

²Sieht man die aussagenlogische Formel als eine Boolesche Funktion spricht man auch von *Variablen*, deshalb der Buchstabe v.

Solver überhaupt startet, weil CNF als Eingabeform erwartet wird? Dies ist nicht der Fall:

9.2 Tseitin-Transformation

Definition 9.1 (Erfüllbarkeitsäquivalenz). Zwei Formeln der Aussagenlogik ϕ und ψ heißen *erfüllbarkeitsäquivalent*, wenn gilt:

$$\phi \text{ erfüllbar} \Leftrightarrow \psi \text{ erfüllbar.}$$

Die *Tseitin*³-Transformation besteht nun darin, eine beliebige Formel ϕ in eine *erfüllbarkeitsäquivalente* Formel in CNF umzuformen. Die Tseitin-Transformation ist linear in der Zahl der Atome der Formel.

```
function TSEITIN( $\phi$ ) {
// post: Eine erfüllbarkeitsäquivalente Formel  $\phi'$  in CNF
```

1. Führe für jede Subformel ψ von ϕ , die kein Atom ist, ein neues Atom T_ψ hinzu.
2. Setze $\phi' = T_\phi$.
3. Durchlaufe den Syntaxbaum von ϕ und füge ϕ' je nach Form der Subformel an einem inneren Knoten die Formel in CNF nach Tabelle 9.1 verbunden mit \wedge hinzu. (Atome werden analog zu den anderen Subformeln behandelt.)

}

Tabelle 9.1: Regeln für die Tseitin-Transformation

$\phi = \neg\phi_1$	$(\neg T_\phi \vee \neg T_{\phi_1}) \wedge (T_\phi \vee T_{\phi_1})$
$\phi = \phi_1 \wedge \phi_2$	$(\neg T_\phi \vee T_{\phi_1}) \wedge (\neg T_\phi \vee T_{\phi_2}) \wedge (T_\phi \vee \neg T_{\phi_1} \vee \neg T_{\phi_2})$
$\phi = \phi_1 \vee \phi_2$	$(T_\phi \vee \neg T_{\phi_1}) \wedge (T_\phi \vee \neg T_{\phi_2}) \wedge (\neg T_\phi \vee T_{\phi_1} \vee T_{\phi_2})$
$\phi = \phi_1 \rightarrow \phi_2$	$(T_\phi \vee T_{\phi_1}) \wedge (T_\phi \vee \neg T_{\phi_2}) \wedge (\neg T_\phi \vee \neg T_{\phi_1} \vee T_{\phi_2})$

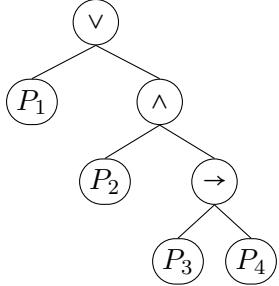
Die Tseitin-Transformation ϕ' einer Formel ϕ hat folgende Eigenschaften:

1. Die Menge der Atome von ϕ ist eine Teilmenge der Atome von ϕ' .
2. Wenn v eine erfüllende Belegung von ϕ ist, dann gibt es eine Erweiterung von v auf die Atome von ϕ' , so dass diese Belegung ϕ' erfüllt.
3. Ist v' eine erfüllende Belegung von ϕ' , dann erfüllt sie auch ϕ .

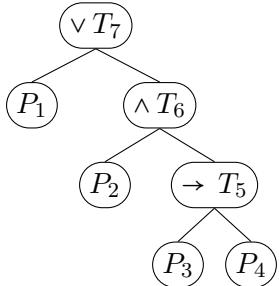
³nach Grigori S. Zeitin, russischer Mathematiker, geb. 1936 [Tse83]

9.2.1 Beispiel

Betrachten wir die Formel $\phi = P_1 \vee (P_2 \wedge (P_3 \rightarrow P_4))$.



Im Schritt 1 legen wir pro Knoten, der nicht Blatt ist, ein neues Atom fest.



Im Schritt 2 erstellen wir ϕ' :

$$\begin{aligned}
 & T_7 \wedge \\
 & (T_7 \vee \neg P_1) \wedge (T_7 \vee \neg T_6) \wedge (\neg T_7 \vee P_1 \vee T_6) \wedge \\
 & (\neg T_6 \vee P_2) \wedge (\neg T_6 \vee T_5) \wedge (T_6 \vee \neg P_2 \vee \neg T_5) \wedge \\
 & (T_5 \vee P_3) \wedge (T_5 \vee \neg P_4) \wedge (\neg T_5 \vee \neg P_3 \vee P_4)
 \end{aligned}$$

9.3 DPLL und CDLC

Definition 9.2 (Wert-Propagation). Sei ϕ eine Formel in CNF und \hat{P} ein Literal. Dann bezeichnet $\phi[\top/\hat{P}]$ die Formel, die dadurch entsteht, dass \hat{P} durch den Wert \top ersetzt wird.

Durch die Wert-Propagation wird die gegebene Formel folgendermaßen vereinfacht:

- Jede Klausel der Formel, die \hat{P} enthält, fällt weg. Denn sie wird durch die Wertzuweisung von \top an \hat{P} wahr.
- In jeder Klausel der Formel, in der $\neg\hat{P}$ vorkommt, entfällt dieser Ausdruck, da er \perp ist und deshalb die Klausel nicht wahr machen kann.

Der Basis-Algorithmus von SAT-Solvern basiert wesentlich auf der Wert-Propagation.

Definition 9.3 (Einzelklausel). Eine Klausel einer Formel in CNF heißt *Einzelklausel*, wenn sie aus genau einem Literal besteht.

Definition 9.4 (Reines Literal). Ein Literal in einer Formel in CNF heißt *reines Literal*, wenn es in allen Klauseln nur als P oder $\neg P$ vorkommt.

Viele SAT-Solver verwenden (stark weiterentwickelte) Varianten des folgenden Algorithmus von Martin Davis⁴, Hilary Putnam⁵, George Logemann⁶ und Donald W. Loveland⁷ ([DP60], [DLL62]).

```

boolean function DPLL( $\phi, \mathcal{M}$ ) {
    // pre:  $\phi$  eine Formel in CNF,  $\mathcal{M}$  eine partielle Belegung
    // return: true falls  $\phi$  erfüllbar ist
    // post: Eine Belegung  $\mathcal{M} = \{\hat{P}_1, \hat{P}_2, \dots\}$  der Aussagensymbole
    // von  $\phi$ , falls  $\phi$  erfüllbar ist
    // modifies:  $\mathcal{M}$ 

    case {
         $\phi = \top$ :
            return true;
         $\phi = \perp$ :
            return false;
         $\phi$  hat eine Einzelklausel ( $\hat{P}$ ):
            return DPLL( $\phi[\top/\hat{P}], \mathcal{M} \cup \hat{P}$ );
         $\phi$  hat ein reines Literal  $\hat{P}$ :
            return DPLL( $\phi[\top/\hat{P}], \mathcal{M} \cup \hat{P}$ );
        otherwise:
            wähle zu einem Atom  $Q$  in der Formel mit  $\hat{Q} \notin \mathcal{M}$ 
            return DPLL( $\phi[\top/Q], \mathcal{M} \cup Q$ )  $\vee$  DPLL( $\phi[\perp/Q], \mathcal{M} \cup \neg Q$ );
    }
}

```

⁴Martin Davis, amerikanischer Logiker und Informatiker, geb. 1928

⁵Hilary Putnam, amerikanischer Philosoph, 1926 - 2016

⁶George Logemann, amerikanischer Mathematiker, 1938 - 2012

⁷Donald W. Loveland, amerikanischer Informatiker, geb. 1934

9.3.1 Idee des Algorithmus

1. Propagation von Einzelklauseln

Besteht eine Klausel nur aus einem Literal, also P oder $\neg P$, dann muss $P = \text{true}$ bzw. $\neg P = \text{true}$ sein, damit die Formel in CNF erfüllbar wird.

Folge: Man kann alle Klauseln weglassen, in denen \hat{P} vorkommt, und außerdem $\neg\hat{P}$ in allen Klauseln, in denen es vorkommt.

2. Elimination von reinen Literalen

Wenn in der Formel nur \hat{P} , niemals aber $\neg\hat{P}$ vorkommt, dann kann man $\hat{P} = \text{true}$ setzen. Denn dadurch fallen alle Klauseln weg, die \hat{P} enthalten, d.h. die Wahl kann niemals zu einem Widerspruch führen, weil ja weder P noch $\neg P$ noch vorkommt.

Folge: Man kann alle Klauseln weglassen, in denen \hat{P} vorkommt, denn sie sind dann erfüllt.

3. Rekursion (*Backtracking*)

Wenn keine der genannten Möglichkeiten bestehen, muss man ein Aussagensymbol Q der Formel ϕ wählen. Es gilt dann natürlich: ϕ erfüllbar $\Leftrightarrow \phi \wedge Q$ erfüllbar oder $\phi \wedge \neg Q$ erfüllbar.

9.3.2 Beispiele

Wir betrachten zunächst das einfache Beispiel der Formel, an der wir den Markierungsalgorithmus für Horn-Formeln demonstriert haben:

$$\begin{aligned} & P \wedge \\ & (\neg P \vee Q) \wedge \\ & (\neg P \vee \neg Q \vee R) \wedge \\ & (\neg P \vee \neg R) \end{aligned}$$

Im ersten Schritt setzt man $P \text{ true}$, da die erste Klausel eine Einzelklausel ist. Die Propagation dieses Werts führt dazu, dass diese Klausel selbst wegfällt und in allen anderen Klauseln $\neg P$ gestrichen werden kann. Man erhält also:

$$\begin{aligned} & Q \wedge \\ & (\neg Q \vee R) \wedge \\ & \neg R \end{aligned}$$

Nun ist Q auf **true** zu setzen und dieser Wert zu propagieren, also folgt:

$$\begin{array}{c} R \wedge \\ \neg R \end{array}$$

Und diese beiden Einzelnklauseln bilden den Widerspruch, d.h. die Formel ist *unerfüllbar*.

Nach diesem einfachen Beispiel, das gezeigt hat, dass der Markierungsalgorithmus im Grunde mit der Idee der Propagation von Einzelnklauseln arbeitet, folgt das Beispiel von 9.1:

ϕ sei wieder die folgende Formel in CNF:

$$\begin{aligned} & (P_1 \vee P_2 \vee P_3) \wedge \\ & (P_1 \vee \neg P_2 \vee \neg P_3) \wedge \\ & \quad (P_1 \vee \neg P_5) \wedge \\ & (\neg P_2 \vee \neg P_3 \vee \neg P_5) \wedge \\ & (\neg P_1 \vee \neg P_2 \vee P_3) \wedge \\ & \quad (P_4 \vee P_6) \wedge \\ & \quad (P_4 \vee \neg P_6) \wedge \\ & \quad (P_2 \vee \neg P_4) \wedge \\ & \quad (\neg P_3 \vee \neg P_4) \end{aligned}$$

Schritt 1 Es gibt keine Einzelnklausel, aber $\neg P_5$ ist ein reines Literal, d.h. wir brauchen für P_5 nur den Fall $\neg P_5 = \text{true}$ zu betrachten.

D.h. $\mathcal{M} = \{\neg P_5\}$ und $\phi[\top/\neg P_5]$ enthält die Klauseln mit $\neg p_5$ nicht mehr, also

$$\begin{aligned} & (P_1 \vee P_2 \vee P_3) \wedge \\ & (P_1 \vee \neg P_2 \vee \neg P_3) \wedge \\ & (\neg P_1 \vee \neg P_2 \vee P_3) \wedge \\ & \quad (P_4 \vee P_6) \wedge \\ & \quad (P_4 \vee \neg P_6) \wedge \\ & \quad (P_2 \vee \neg P_4) \wedge \\ & \quad (\neg P_3 \vee \neg P_4) \end{aligned}$$

Schritt 2 Probiere $P_1 = \text{true}$, also $\mathcal{M} = \{\neg P_5, P_1\}$. Die Klauseln mit P_1 sind **true** und in den Klauseln mit $\neg P_1$ kann man $\neg P_1$ weglassen. Dann bleibt

$$\begin{aligned} & (\neg P_2 \vee P_3) \wedge \\ & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (P_2 \vee \neg P_4) \wedge \\ & (\neg P_3 \vee \neg P_4) \end{aligned}$$

Schritt 3 Probiere $P_2 = \text{true}$, also $\mathcal{M} = \{\neg P_5, P_1, P_2\}$. Die Klauseln mit P_2 sind **true** und in den Klauseln mit $\neg P_2$ kann man $\neg P_2$ weglassen. Dann bleibt

$$\begin{aligned} & (P_3) \wedge \\ & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (\neg P_3 \vee \neg P_4) \end{aligned}$$

(P_3) ist nun eine Einzelklausel, d.h. P_3 muss **true** sein, also $\mathcal{M} = \{\neg P_5, P_1, P_2, P_3\}$. Es bleibt:

$$\begin{aligned} & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (\neg P_4) \end{aligned}$$

$(\neg P_4)$ ist nun auch Einzelklausel, und es bleibt:

$$\begin{aligned} & (P_6) \wedge \\ & (\neg P_6) \end{aligned}$$

Dies ist aber der Widerspruch.

Schritt 4 Probiere $P_2 = \text{false}$, also $\mathcal{M} = \{\neg P_5, P_1, \neg P_2\}$. Dann bleibt

$$\begin{aligned} & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (\neg P_4) \wedge \\ & (\neg P_3 \vee \neg P_4) \end{aligned}$$

$(\neg P_4)$ ist jetzt Einzelklausel, d.h. P_4 muss **false** sein, d.h.

$$\begin{aligned} & (P_6) \wedge \\ & (\neg P_6) \wedge \\ & (\neg P_3) \end{aligned}$$

Erneut der Widerspruch.

Schritt 5 Probiere $P_1 = \text{false}$, also $\mathcal{M} = \{\neg P_5, \neg P_1\}$. Dann bleibt:

$$\begin{aligned} & (P_2 \vee P_3) \wedge \\ & (\neg P_2 \vee \neg P_3) \wedge \\ & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (P_2 \vee \neg P_4) \wedge \\ & (\neg P_3 \vee \neg P_4) \end{aligned}$$

Schritt 5 Probiere $P_2 = \text{true}$, also $\mathcal{M} = \{\neg P_5, \neg P_1, P_2\}$. Dann bleibt:

$$\begin{aligned} & (\neg P_3) \wedge \\ & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \wedge \\ & (\neg P_3 \vee \neg P_4) \end{aligned}$$

$(\neg P_3)$ ist jetzt Einzelklausel, d.h. P_3 muss **false** sein, also $\mathcal{M} = \{\neg P_5, \neg P_1, P_2, \neg P_3\}$. Dann bleibt:

$$\begin{aligned} & (P_4 \vee P_6) \wedge \\ & (P_4 \vee \neg P_6) \end{aligned}$$

P_4 ist jetzt reines Literal, d.h. P_4 muss **true** sein, dann bleibt nichts mehr übrig, alle Klauseln sind erfüllt. D.h. die Wahl der Belegung für P_6 ist beliebig.

Ergebnis $\mathcal{M} = \{\neg P_5, \neg P_1, P_2, \neg P_3, P_4, P_6\}$ ist eine erfüllende Belegung.

9.3.3 Von DPLL zu CDLC

Der vorgestellte DPLL-Algorithmus gibt die Idee wieder, heutige SAT-Solver verwenden verbesserte Algorithmen mit folgenden Eigenschaften:

1. Oft wird keine Analyse bezüglich reiner Literale gemacht, weil diese Analyse aufwändig ist.

2. Stattdessen wird im Fall eines *Konflikts* genau analysiert, wodurch er entstanden ist und eine neue Klausel hinzugefügt, die dazu führt, dass der Algorithmus einmal gefundene Abhängigkeiten zwischen Atomen nicht „vergisst“ und deshalb erneut auswerten muss.

Die Idee kann man an unserem Beispiel oben sehen. Wir haben in Schritt 1 P_1 als `true` und in Schritt 2 P_2 als `true` gewählt. Diese beiden Entscheidungen haben zum Widerspruch geführt. Also muss gelten: $\neg p_1 \vee \neg p_2$. Diese Klausel können wir nun unserer ursprünglichen Formel hinzufügen. Der Algorithmus hat aus dem Konflikt „gelernt“.

Klausel-lernende SAT-Solver werden auch CDLC-Solver (*Conflict Driven Clause Learning*) genannt.

3. Diese Analyse kann noch weitergehen: Man merkt sich in welchem Level der Analyse man eine Entscheidung getroffen hat und macht bei einem Konflikt nicht einfach *Backtracking*, sondern *Backjumping*.

4. Außerdem werden Heuristiken eingesetzt, welche Variable beim Backjumping „ausprobiert“ wird. Ein Beispiel wäre etwa: DLCS (*Dynamic Largest Combined Sum*) – man wählt die Variable, die positiv oder negativ am häufigsten in der Formel vorkommt.

Würde man diese Strategie in unserem Beispiel verwenden, müsste man in Schritt 2 mit $P_2 = \text{true}$ starten, danach P_3 mit `true` probieren, was zum Konflikt führt. Doch $P_3 = \text{false}$ führt zu einer erfüllenden Belegung. Wir wären also etwas schneller.

Wie aktuelle SAT-Solver arbeiten wird in [KS06] und [Knu15] beschrieben.

Kapitel 10

Anwendungen der Aussagenlogik in der Softwaretechnik

In der Programmierung spielt die Aussagenlogik eine prominenten Rolle, wenn immer Bedingungen zu formulieren sind, also etwa bei bedingten Anweisungen oder Fallunterscheidungen. In diesem Kapitel werfen wir einen kurzen Blick auf einige andere Anwendungen der Aussagenlogik und von SAT-Solvern in der Softwaretechnik.

10.1 Anwendungen von SAT-Techniken

Einige Beispiele für den Einsatz von SAT-Solvern, um nicht-triviale Fragestellungen zu lösen.

- 2003 – Validierung von Produktkonfigurationen in der Automobilindustrie, Carsten Sinz et al, siehe [SKK03].
- 2009 – Formale Verifizierung des Intel Core 7 Prozessors, Kaivola et al, siehe [KGN⁺09]
- 2010 – Verifikation von Windows 7 Gerätetreibern mit einem SMT-Solver, De Moura, Bjørner, siehe [dMB10]. SMT (SAT modulo Theory) baut auf dem Konzept von SAT-Solvern auf. Microsoft Research hat einen SMT-Solver namens Z3 entwickelt, siehe <https://github.com/Z3Prover/z3/wiki>.
- 2014 – Analyse der Terminierung von Programmen, Jürgen Giesl et al, siehe [GBE⁺14].
- 2016/18 – Management von Abhängigkeiten innerhalb des Ökosystems der Eclipse Plattform, Le Berre, Rapicault, siehe [BR18].
- ...

10.2 Statische Codeanalyse

Das folgende Beispiel ist aus [KS06, Example 2.2], von mir zu einer kleinen Geschichte ausgebaut.

Bei einem Codereview richtet sich das Auge des Reviewers auf folgendes Codestück:

```
if (!a && !b) h();
else if (!a) g();
else f();
```

Der Entwickler versichert, dass der Code getestet wurde und in alle Testfällen das gewünschte Ergebnis zur Folge hatte. Gleichwohl ist der Reviewer der Auffassung, dass dieses Codestück doch einfacher und damit für Menschen verständlicher geschrieben werden können müsste. Etwas unwillig erklärt sich der Entwickler dazu bereit und kommt am kommenden Tag wieder.

Er bringt zwei Fassungen mit:

Version 1:

```
if (a) h();
else if (b) g();
else f();
```

Version 2:

```
if (a) f();
else if (b) g();
else h();
```

und richtet milde lächelnd die Frage an den Reviewer: „Und welche der Versionen sollen wir nun nehmen?“

Der Reviewer freilich kennt seine Aussagenlogik und übersetzt die ursprüngliche Fassung sowie die beiden neuen Versionen indem er die Terme der Bedingungen sowie die Funktionen zu Aussagensymbolen macht:

Original:

```
if ( $\neg a \wedge \neg b$ ) then  $h$ 
else if ( $\neg a$ ) then  $g$ 
else  $f$ 
```

Version 1 (2 analog):

```
if  $a$  then  $h$ 
else if  $b$  then  $g$ 
else  $f$ 
```

Nun muss man nur noch **if-then-else** in eine Formel transformieren:

$$\text{if } x \text{ then } y \text{ else } z \rightsquigarrow (x \wedge y) \vee (\neg x \wedge z)$$

Und schon hat man drei Formeln:

$$\begin{aligned}\phi_{orig} &\hat{=} ((\neg a \wedge \neg b) \wedge h) \vee (\neg(\neg a \wedge \neg b) \wedge (\neg a \wedge g) \vee (a \wedge f)) \\ \phi_{v_1} &\hat{=} (a \wedge h) \vee (\neg a \wedge ((b \wedge g) \vee (\neg b \wedge f))) \\ \phi_{v_2} &\hat{=} (a \wedge f) \vee (\neg a \wedge ((b \wedge g) \vee (\neg b \wedge h)))\end{aligned}$$

Jetzt kann man einen SAT-Solver verwenden, um zu überprüfen, ob $\phi_{orig} \leftrightarrow \phi_{v_1}$ oder $\phi_{orig} \leftrightarrow \phi_{v_2}$ gilt.

Mit der Logic Workbench kann man sich die Sache noch einfacher machen, weil es in ihr den dreistelligen Operator `ite` gibt:

```
; Originaler Code
(def orig '(ite (and (not a) (not b)) h (ite (not a) g f)))
; Version 1
(def vers1 '(ite a h (ite b g f)))
; Version 2
(def vers2 '(ite a f (ite b g h)))

; Was ist richtig?
(valid? (list 'equiv orig vers1))
; => false
(valid? (list 'equiv orig vers2))
; => true
```

10.3 Featuremodelle für (Software-)Produktlinien

In der Softwareentwicklung kommt es nicht selten vor, dass verwandte Anwendungen entwickelt werden, die Gemeinsamkeiten, aber auch Unterschiede haben. Wenn man dies auf *systematische* Weise tut, dann spricht man von einer *Softwarereproduktlinie*.

Die systematische Analyse von Gemeinsamkeit und Variabilität innerhalb einer Softwarereproduktlinie wird mittels *Feature-Modellierung* durchgeführt. Die Eigenschaften der verschiedenen Produkte in einer Produktlinie werden als *Features* bezeichnet.

Die *Features* werden im Feature-Modell in einem Baum angeordnet, wobei verschiedene Arten von Kanten zwischen Super- und Subfeatures die Variabilität beschreiben. Außerdem gibt es Integritätsbedingungen, die über Zweige des Baums hinweggehen, sogenannte *Cross Tree Constraints* (CTCs). Der Feature-Baum zusammen mit den CTCs ergibt das Feature-Modell.

Eine Auswahl von Features, die alle Bedingungen im Feature-Modell erfüllt, wird als eine gültige *Konfiguration* bezeichnet. Können noch weitere Features gewählt werden, spricht man von einer *partiellen* Konfiguration, besteht keine Wahlmöglichkeit mehr von einer *vollständigen* Konfiguration.

Typischerweise werden in Feature-Modelle folgende vier Arten der Beziehungen zwischen Super- und Subfeatures unterschieden:

- ① Ein Subfeature ist *obligatorisch*, d.h. wenn das Superfeature in einer Konfiguration gewählt wird, dann ist das Subfeature automatisch auch gewählt.
- ② Ein Subfeature ist *optional*, d.h. wenn das Superfeature in einer Konfiguration gewählt wird, dann kann das Subfeature gewählt werden oder auch nicht.
- ③ Eine Gruppe von Subfeatures wird als *Oder-Gruppe* dargestellt, wenn die Wahl des Superfeatures erzwingt, dass mindestens eines der Subfeatures gewählt werden muss.
- ④ Eine Gruppe von Subfeatures wird als *Alternativ-Gruppe* dargestellt, wenn die Wahl des Superfeatures erzwingt, dass genau eines der Subfeatures gewählt werden muss.

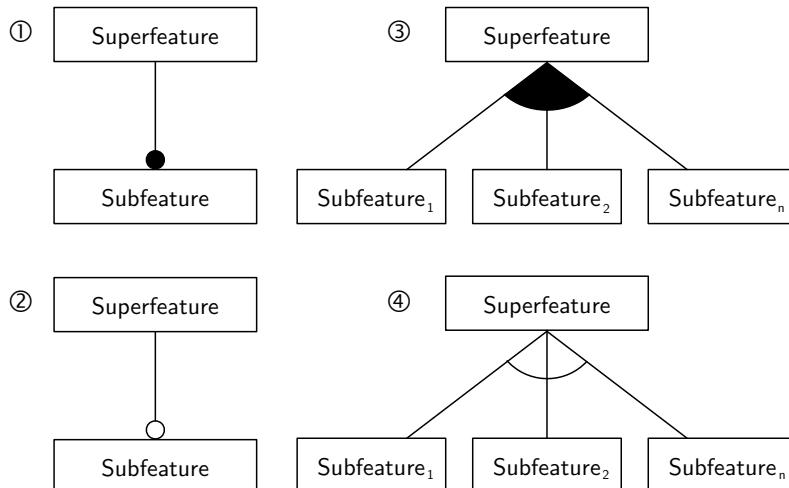


Abbildung 10.1: Beziehungen im Feature-Baum

Abbildung 10.1 stellt dar, wie diese vier Beziehungen im Feature-Diagramm graphisch dargestellt werden.

Die Integritätsbedingungen zwischen beliebigen Features unabhängig von der Baumstruktur, die CTCs, werden als aussagenlogische Formeln ausgedrückt, wobei die Features die Aussagensymbole sind. (Das setzt voraus, dass die Bezeichnungen der Features im Baum eindeutig sind.)

Die Featuremodellierung wurde als Bestandteil der *Feature Oriented Domain Analysis* (FODA) 1990 von Kyo C. Kang et al. beim Software Engineering Institute SEI eingeführt [KCH⁺90]. Seither wurden viele Varianten des Feature-Modells entwickelt, einen Überblick findet man

in [MH07]. Ich verwende die Notation, die in der FeatureIDE, einem Werkzeug der Feature-Modellierung, eingesetzt wird, siehe [ABKS13] und [MTS⁺17].

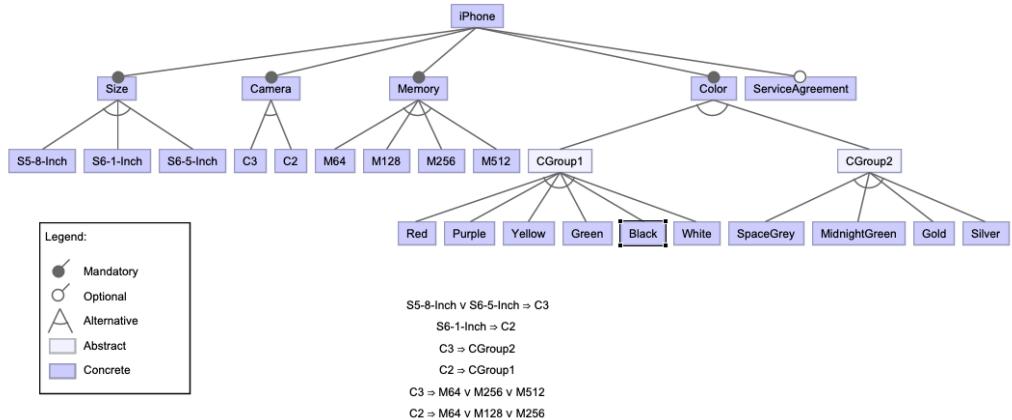


Abbildung 10.2: Feature-Modell für das iPhone

Abbildung 10.2 zeigt ein Feature-Modell für die Varianten des iPhones 2019. Das Modell wurde in FeatureIDE (siehe <https://featureide.github.io> und [MTS⁺17]) erstellt. In der Legende werden Features nach *abstract* und *concrete* unterschieden. Abstrakte Features dienen der Strukturierung des Feature-Baums, sie sind als solche nicht im Produkt konkret auffindbar. Die Aussagen unterhalb des Baums sind die CTCs.

Was nun hat das Feature-Modell mit der Aussagenlogik zu tun? Wir nehmen die Features als Aussagensymbole und verstehen zugeordnete Wahrheitswerte als Festlegungen, ob das Feature für die zu treffende Konfiguration gewählt wurde (also T ist) oder nicht (also F ist).

Das Feature-Modell entspricht auf diese Weise einer Formel der Aussagenlogik, die als Konjunktion folgender Teilformel gebildet wird:

- Jede mögliche Konfiguration soll ja tatsächlich ein Produkt definieren, dessen Varianten im Modell beschrieben werden. Das bedeutet, dass die Wurzel *Root* des Baums T sein muss, d.h. *Root* ist eine Teilformel:

$$\text{Root}$$

- Bei obligatorischen Subfeatures besteht eine logische Äquivalenz zum Superfeature: Ist das Superfeature *Super T*, dann muss auch das Subfeature *oblSub T* sein. Und wenn das Subfeature T ist, dann

ist das nur möglich, wenn das Superfeature gewählt ist, also

$$oblSub \leftrightarrow Super$$

- Beim optionalen Subfeature $optSub$ ist dieses bei Wahl des Super nicht zwingend erforderlich, also

$$optSub \rightarrow Super$$

- Bei einer Oder-Gruppe von Subfeatures $oSub_1, oSub_2, \dots, oSub_n$ gilt

$$oSub_1 \vee oSub_2 \vee \dots \vee oSub_n \leftrightarrow Super$$

- Bei einer Alternativ-Gruppe $aSub_1, aSub_2, \dots, aSub_n$ muss exakt eines der Subfeatures der Wahl des Superfeatures entsprechen:

$$(aSub_1 \vee aSub_2 \vee \dots \vee aSub_n) \wedge \bigwedge_{i < j} (\neg aSub_i \vee \neg aSub_j) \leftrightarrow Super$$

- Cross Tree Constraints werden der Formel einfach hinzufügt.

Auf diese Weise (zuerst beschrieben in [Bat05]) entspricht ein Feature-Modell gerade einer Formel der Aussagenlogik und die erfüllenden Belegungen der Formel sind gerade die möglichen vollständigen Konfigurationen von Varianten.

Das bereits erwähnte Werkzeug FeatureIDE verwendet diese Korrespondenz und setzt den SAT-Solver SAT4J ein, um Feature-Modelle zu analysieren und Modellierer zu unterstützen.

Teil II

Prädikatenlogik

Kapitel 11

Objekte und Prädikate

Die Ausdruckskraft der Aussagenlogik ist beschränkt. Wir werden folgenden Schluss sicherlich für richtig halten:

Alle Quadratzahlen $\neq 0$ sind positiv (P)

16 ist eine Quadratzahl (Q)

Also folgt: 16 ist positiv (R)

Übertragen wir diesen Schluss etwas naiv in die Aussagenlogik, so ergibt sich $P \wedge Q \rightarrow R$ — und es gibt keinerlei Grund anzunehmen, dass diese Aussage zutrifft.

Dies liegt daran, dass wir in der Aussagenlogik den Zusammenhang zwischen der ersten und der zweiten Aussage nicht erfassen können, nämlich, dass die 16 ein Exemplar von der Sorte *Quadratzahl* ist.

Also: Wir müssen unterscheiden können zwischen

Objekten, den Dingen eines Universums, einer „Welt“, wie z.B. Zahlen, Strings, Werten, Objekten usw. und

Prädikaten, Aussagen über die Objekte, die wahr oder falsch sein können.

Beispiel Ist etwa unser Universum die Welt der ganzen Zahlen \mathbb{Z} , dann könnten wir folgende Prädikate haben

$Sq(x)$ bedeutet „ x ist eine Quadratzahl $\neq 0$ “

$Pos(x)$ bedeutet „ x ist positiv“

Dann können wir das einleitende Beispiel so ausdrücken

$$\forall x(Sq(x) \rightarrow Pos(x)) \wedge Sq(16) \rightarrow Pos(16)$$

11.1 Elemente der Sprache der Prädikatenlogik

Gegeben sei stets eine Menge \mathbb{U} , das Universum, auch genannt „Miniwelt“. In der Regel wird in der Literatur vorausgesetzt, dass das Universum nicht leer ist, d.h. $\mathbb{U} \neq \emptyset$ ¹

Wir verwenden zusätzlich zu den Junktoren der Aussagenlogik

Variablen

$x, y, z \dots$

Variablen sind Platzhalter für beliebige Objekte des Universums, z.B. steht in $Sq(x)$ die Variable x für ein Element des Universums, also in unserem Beispiel für eine Zahl in \mathbb{Z} .

Konstanten

$c, d, e \dots$

Konstanten sind bestimmte, benannte Elemente des Universums, z.B. 16, die Zahl $16 \in \mathbb{Z}$.

Funktionen

$f, g, h \dots$

Funktionen operieren auf den Elementen des Universums und ergeben wieder Elemente des Universums, z.B. $plus(16, 9)$ ergibt das Element $25 \in \mathbb{Z}$ mit der naheliegenden Definition von $plus$.

Prädikate

$P, Q, R \dots$

Prädikate sind Boolesche Funktionen, die Aussagen über Elemente der Welt machen. Die Wertemenge eines Prädikats ist also in $\mathbb{B} = \{\text{T}, \text{F}\}$. In unserem Beispiel ist Sq ein Prädikat der Arität 1, $Sq(x)$ ist genau dann wahr, wenn $x \in \mathbb{Z}$ eine Quadratzahl ist.

Gleichheit

$=$

Gleichheit ist ein spezielles Prädikat, das wir in die Sprache von vorneherein aufnehmen.²

¹Ist das Universum leer, dann ist jede Aussage der Form $\exists x \dots$ immer falsch und eine der Form $\forall x \dots$ immer wahr – diese Fälle möchte man gerne vermeiden.

²Man kann auch Prädikatenlogik ohne Gleichheit machen, für Anwendungen ist es jedoch nützlich, die Gleichheit als *logisches* Symbol aufzufassen.

Quantoren

$$\forall x\phi, \exists y\phi$$

Quantoren machen Aussagen über *alle* Elemente des Universums oder darüber, ob ein Element des Universums mit einer bestimmten Eigenschaft *existiert*.

11.2 Prädikate und Relationen

Es besteht eine wichtige grundlegende Beziehung zwischen *Prädikaten und Relationen*:

Sei R eine n -wertige Relation über \mathbb{U} , d.h. $R \subset \mathbb{U}^n$. Dann kann man diese Relation repräsentieren durch die Boolesche Funktion $r : \mathbb{U}^n \rightarrow \mathbb{B}$ definiert durch

$$r(a_1, \dots, a_n) = T \text{ genau dann, wenn } (a_1, \dots, a_n) \in R$$

Ist etwa $Sq \subset \mathbb{Z} = \{x / \exists y \text{ mit } x = y^2 \text{ und } x > 0\}$, also

$$Sq = \{1, 4, 9, 16, 25, \dots\}$$

dann entspricht diese einstellige Relation gerade dem oben verwendeten Prädikat Sq .

Offenbar sind also Prädikate und Relationen austauschbare Konzepte, deshalb spricht man bei der Prädikatenlogik erster Ordnung auch manchmal von *relationaler Logik*.

Bemerkung Man könnte in unserem Beispiel auch eine binäre Relation $Sq \subset \mathbb{N}^2$ auf folgende Weise definieren:

Sei $square : \mathbb{N} \rightarrow \mathbb{N}$ die Funktion, die einem $x \in \mathbb{N}$ sein Quadrat als Funktionswert zuordnet, also $x \mapsto x^2$. Diese Funktion kann man als binäre Relation auffassen, nämlich $Sq = \{(x, x^2) / x \in \mathbb{N}\}$. Ein Tupel (x, y) ist also genau dann in Sq , wenn y das Quadrat von x ist. Auf diese Weise entspricht jeder n -stellige Funktion eine $n + 1$ -stellige Relation.

Kapitel 12

Die formale Sprache der Prädikatenlogik

12.1 Signatur, Terme, Formeln

In der Sprache der Prädikatenlogik verwendet man Funktions- und Konstantensymbole sowie Prädikatssymbole. Genau genommen bezieht man sich auf eine bestimmte Wahl dieser Symbole und spricht dann von *einer Sprache* \mathcal{L} der Prädikatenlogik.

Definition 12.1 (Signatur). Die *Signatur* einer Sprache \mathcal{L} besteht aus einer Menge von Prädikatssymbolen $\{P_1, \dots, P_n\}$, von Funktionssymbolen $\{f_1, \dots, f_m\}$ und von Konstantensymbolen $\{c_1, \dots, c_k\}$.

Man schreibt die Signatur so:

$$\{P_1^{r_1}, \dots, P_n^{r_n}; f_1^{a_1}, \dots, f_m^{a_m}; c_1, \dots, c_k\}$$

wobei die r und die a die Arität der Prädikatssymbole bzw. Funktionssymbole bezeichnet.

Bemerkungen

- Die Signatur besteht aus den „nicht-logischen“ Symbolen der Sprache \mathcal{L} .
- Manche Autoren definieren die Signatur dadurch, dass sie nur die Arität von Prädikatssymbolen, Funktionssymbolen und die Zahl der Konstanten angeben. Denn „Name ist Schall und Rauch“¹. In dieser Sicht wird die Signatur so angegeben:

$$< r_1, \dots, r_n; a_1, \dots, a_m; k >$$

¹J.W. von Goethe, Faust I, Marthens Garten

wobei r_i die Arität eines Prädikatensymbols, a_i die Arität eines Funktionssymbols und k die Zahl der Konstanten ist.

- Man kann Konstantensymbole auch als Funktionssymbole der Arität 0 auffassen.
- Prädikatssymbole der Arität 0 kann man als Aussagensymbole auffassen. Oder anders: Wenn in der Signatur nur Prädikatssymbole der Arität 0 vorkommen und keine anderen Symbole und wir uns auf die Junktoren $\neg, \wedge, \vee, \rightarrow$ beschränken, dann erhalten wir gerade die Definition einer Sprache der Aussagenlogik, wie in Teil I.

Im Folgenden sei eine Signatur gegeben, sowie eine Menge von Variablen $\{x, y, \dots\}$.

Definition 12.2 (Terme). Die *Terme* sind Zeichenketten, die nach folgenden Regeln gebildet werden:

- (i) Jede Variable ist ein Term.
- (ii) Jedes Konstantensymbol ist ein Term.
- (iii) Sind t_1, \dots, t_n Terme und f ein Funktionssymbol mit der Arität n , dann ist auch $f(t_1, \dots, t_n)$ ein Term.

Als *Grammatik* in Backus-Naur-Darstellung können wir diese Regeln so ausdrücken:

$$t ::= x \mid c \mid f \mid f(t, \dots, t)$$

mit Variablen x , Konstantensymbolen c und Funktionssymbolen f .

Definition 12.3 (Formeln). Die *Formeln* sind die Zeichenketten, die durch folgende Regeln generiert werden können:

- (i) \perp ist eine Formel (genannt: der Widerspruch) und \top ist eine Formel (genannt: die Wahrheit).
- (ii) Ist P ein Prädikatssymbol der Arität 0, dann ist P eine Formel.
Ist P ein Prädikatssymbol der Arität $n \geq 1$ und sind t_1, \dots, t_n Terme, dann ist $P(t_1, \dots, t_n)$ eine Formel.
Sind t_1 und t_2 Terme, dann ist $(t_1 = t_2)$ eine Formel.
- (iii) Ist ϕ eine Formel, dann auch $(\neg\phi)$.
Sind ϕ und ψ Formeln, dann auch $(\phi \wedge \psi)$, $(\phi \vee \psi)$ und $(\phi \rightarrow \psi)$.
- (iv) Ist ϕ eine Formel und x eine Variable, dann sind $\forall x \phi$ und $\exists x \phi$ Formeln.

In Backus-Naur-Darstellung:

$$\begin{aligned}\phi ::= & \perp \mid \top \mid P \mid P(t, \dots, t) \mid (t = t) \mid \\ & (\neg\phi), \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \rightarrow \phi) \mid \\ & \forall x \phi \mid \exists x \phi\end{aligned}$$

mit Termen t , Variablen x und Prädikatssymbolen P .

Bemerkungen

- Die Argumente von Prädikatssymbolen dürfen *nur* Terme sein, keine anderen Prädikate – wir definieren hier nämlich die Prädikatenlogik *erster* Stufe.
- In unserer Definition der Sprachen der Prädikatenlogik, haben wir die Gleichheit = als *logisches* Symbol mit aufgenommen. In vielen Büchern wird unterschieden zwischen der Prädikatenlogik und der Prädikatenlogik mit Gleichheit.

Man könnte denken, dass man die Gleichheit einfach dadurch einführen kann, dass man ein Prädikatsymbol für die Gleichheit definiert und dabei verlangt, dass in jedem Modell der Sprache dieses gerade die Identitätsrelation über dem Universum des Modells ist.
(Vorgriff – siehe Abschnitt 13.1) [Hof11, S.114f]

Bindungsregeln

$\neg, \forall x, \exists x$ binden am stärksten, dann
 \wedge und \vee (linksassoziativ) und schließlich
 \rightarrow (rechtsassoziativ.)

Diese Bindungsregeln erlauben uns, sparsamer (und dadurch besser lesbar) mit Klammern umzugehen, ohne die Grammatik mehrdeutig zu machen.

12.2 Freie und gebundene Variablen

Sei ϕ eine Formel der Prädikatenlogik. Ein Vorkommen der Variablen x in ϕ heißt *frei*, wenn x im Syntaxbaum nicht Abkömmling eines Quantorknotens $\forall x$ oder $\exists x$ ist. Andernfalls heißt das Vorkommen *gebunden*.

Die Namen von gebundenen Variablen spielen keine Rolle, deshalb werden Formeln, die sich nur durch den Namen gebundener Variablen unterscheiden, identifiziert. $\forall x P(x, y)$ ist also dieselbe Formel wie $\forall z P(z, y)$, nicht jedoch $\forall x P(x, z)$, da die Bedeutung der freien Variablen vom Kontext abhängt.

Definition 12.4 (Satz). Eine Formel ϕ , die keine freien Variablen hat, heißt *Satz* oder *geschlossene Formel*.

Definition 12.5 (Grundterm). Ein Term t , der keine Variablen hat, heißt *geschlossener Term* oder *Grundterm*.

Bemerkung

Hat eine Formel freie Variablen, dann macht man sie zu einem Satz, in dem man sich alle freien Variablen durch den Allquantor gebunden denkt.

12.3 Substitution

Variablen sind Platzhalter für Terme. Substitution besteht darin, solche Platzhalter durch Terme zu ersetzen.

Ein Ersetzen von Variablen durch Terme ist nur möglich für Variablen, die *nicht* durch einen Quantor gebunden sind. Gebundene Variablen stehen für ein bestimmtes Element des Universums oder für alle Elemente des Universums, können somit nicht durch den Term ersetzt werden.

Definition 12.6 (Substitution). Gegeben eine Variable x und ein Term t . Die Formel $\phi[t/x]$ ist die Formel, die aus ϕ entsteht, in dem jedes *freie* Vorkommen von x durch t ersetzt wird.

Dabei darf der eingesetzte Term t keine Variablen enthalten, die durch die Substitution in den Geltungsbereich eines Quantors kommen würden.

Die einschränkende Bemerkung zur Substitution sei an einem Beispiel erläutert:

Haben wir die Formel $\forall xP(x, y)$ und wollen y durch den Term $f(x)$ ersetzen, dann ergäbe sich durch einfaches Einsetzen $\forall xP(x, f(x))$ und plötzlich ist die Variable x im Term $f(x)$ in den Bereich des Allquantors gekommen. Dies ist nicht erlaubt.

Richtig wäre es, zunächst die gebundene Variable umzubenennen, also etwa $\forall zP(z, y)$, wodurch sich die Formeln nicht ändert. Jetzt ist die Substitution möglich:

$(\forall xP(x, y))[f(x)/y]$ ergibt $\forall zP(z, f(x))$, nicht aber $\forall xP(x, f(x))$.

Man sagt, dass eine Term t frei ist für eine Variable x in einer Formel ϕ , wenn t keine Variable enthält, die beim Einsetzen für x in den Geltungsbereich eines Quantors käme.

Bei einer Substitution muss man also erst prüfen, ob der zu substituierende Term frei für die Variable in der Formel ist. Ist dies nicht der Fall, muss man gebundene Variablen in der Formel so umtaufen, dass keine „Kollision“ auftritt.

Bemerkung In der Logic Workbench (lwb) hat man als Junktoren die Junktoren aus der Aussagenlogik, siehe Tabelle 3.1, darüber hinaus:

- das ausgezeichnete Symbol $=$ für die Gleichheit,
- den Allquantor, z.B. `(forall [x y] (and (P x) (Q y)))` mit unären Prädikaten P und Q sowie
- den Existenzquantor, z.B. `(exists [x] (= (f x) (g x)))` mit den unären Funktion f und g .

Kapitel 13

Semantik der Prädikatenlogik

13.1 Modell/Struktur

Definition 13.1 (Modell/Struktur). Ein *Modell* für die Sprache \mathcal{L} ist ein Paar $\mathcal{M} = \langle \mathbb{U}, I \rangle$ mit einer nicht-leeren Menge \mathbb{U} und einer Funktion I , die jedem Symbol in \mathcal{L} eine Interpretation zuordnet nach folgenden Regeln:

- (i) Ist P ein 0-äres Prädikatensymbol, dann ist $I(P)$ ein Wahrheitswert.
- (ii) Ist P ein n -äres Prädikatensymbol für $n > 0$, dann ist $I(P) \subseteq \mathbb{U}^n$ eine n -äre Relation über \mathbb{U} .
- (iii) Ist c ein Konstantensymbol, dann ist $I(c) \in \mathbb{U}$, ein Element von \mathbb{U} .
- (iv) Ist f ein Funktionssymbol mit Arität n , dann ist $I(f) : \mathbb{U}^n \rightarrow \mathbb{U}$ eine Funktion.

Man nennt Modelle der Prädikatenlogik auch spezifischer *Strukturen*.

Die Menge \mathbb{U} nennt man auch das Universum. Die Interpretation schreibt man auch oft so:

- $P^{\mathcal{M}}$ für die Prädikate über \mathbb{U}
- $c^{\mathcal{M}}$ für die Elemente zu den Konstantensymbolen und
- $f^{\mathcal{M}}$ für die Funktionen zu den Funktionssymbolen

Definition 13.2 (Variablenbelegung). Sei $\mathcal{M} = \langle \mathbb{U}, I \rangle$ eine Struktur für \mathcal{L} . Eine *Variablenbelegung* in \mathcal{M} ist eine Funktion l , die jeder Variablen x einen Wert $l(x) \in \mathbb{U}$ zuordnet.

Man schreibt $l[x \mapsto a]$ für die Variablenbelegung, die x auf a abbildet und alle anderen Variablen auf $l(y)$, d.h.

$$l[x \mapsto a](y) = \begin{cases} a & \text{falls } y = x. \\ l(y) & \text{falls } y \neq x. \end{cases}$$

Definition 13.3 (Interpretation der Terme). Sei $\mathcal{M} = \langle \mathbb{U}, I \rangle$ eine Struktur für \mathcal{L} und l eine Variablenbelegung. Für einen Term t von \mathcal{L} definiert man die Interpretation $I(t)$ bezüglich \mathcal{M} und der Variablenbelegung l induktiv über die Länge des Terms durch

- (i) $I(x) := l(x)$ für die Variablen x ,
- (ii) $I(c) := I(c)$ für die Konstanten c , und
- (iii) $I(f(t_1, \dots, t_n)) := I(f)(I(t_1), \dots, I(t_n))$ für die Funktionen f .

Definition 13.4 (Interpretation der Formeln). Sei $\mathcal{M} = \langle \mathbb{U}, I \rangle$ eine Struktur für \mathcal{L} und l eine Variablenbelegung, dann ist \mathcal{M} ein Modell für eine Formel ϕ , geschrieben

$$\mathcal{M} \models_l \phi \quad \text{für die Formel } \phi,$$

falls $\llbracket \phi \rrbracket_l^{\mathcal{M}} = T$. Dabei wird $\llbracket \phi \rrbracket_l^{\mathcal{M}}$ induktiv definiert über den strukturellen Aufbau von ϕ :

(i)	$\llbracket P(t_1, \dots, t_n) \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } (I(t_1), \dots, I(t_n)) \in P^{\mathcal{M}} \\ \text{F sonst} \\ \text{bzw. } I(P) \text{ falls } P\text{-är} \end{cases}$
(ii)	$\llbracket s = t \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } I(s) = I(t) \\ \text{F sonst} \end{cases}$
(iii)	$\llbracket \neg \phi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } \llbracket \phi \rrbracket_l^{\mathcal{M}} = \text{F} \\ \text{F sonst} \end{cases}$
(iv)	$\llbracket \phi \wedge \psi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } \llbracket \phi \rrbracket_l^{\mathcal{M}} = \text{T} \text{ und } \llbracket \psi \rrbracket_l^{\mathcal{M}} = \text{T} \\ \text{F sonst} \end{cases}$
(v)	$\llbracket \phi \vee \psi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } \llbracket \phi \rrbracket_l^{\mathcal{M}} = \text{T} \text{ oder } \llbracket \psi \rrbracket_l^{\mathcal{M}} = \text{T} \\ \text{F sonst} \end{cases}$
(vi)	$\llbracket \phi \rightarrow \psi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls } \llbracket \phi \rrbracket_l^{\mathcal{M}} = \text{F} \text{ oder } \llbracket \psi \rrbracket_l^{\mathcal{M}} = \text{T} \\ \text{F sonst} \end{cases}$
(vii)	$\llbracket \forall x \phi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls für alle } a \in \mathbb{U} \text{ gilt: } \llbracket \phi \rrbracket_{l[x \mapsto a]}^{\mathcal{M}} = \text{T} \\ \text{F sonst} \end{cases}$
(viii)	$\llbracket \exists x \phi \rrbracket_l^{\mathcal{M}}$	$:= \begin{cases} \text{T falls es existiert ein } a \in \mathbb{U} \text{ mit: } \llbracket \phi \rrbracket_{l[x \mapsto a]}^{\mathcal{M}} = \text{T} \\ \text{F sonst} \end{cases}$
(ix)	$\llbracket \top \rrbracket_l^{\mathcal{M}}$	$:= \text{T}$
(x)	$\llbracket \perp \rrbracket_l^{\mathcal{M}}$	$:= \text{F}$

13.2 Semantische Folgerung und Äquivalenz

Definition 13.5 (Semantische Folgerung). Sei Γ eine Menge prädikatenlogischer Formeln und ϕ eine prädikatenlogische Formel. Man sagt:

$\Gamma \models \phi$ d.h. ϕ folgt semantisch aus Γ , genau dann wenn jedes Modell für Γ auch ein Modell für ϕ ist.

Besteht Γ nur aus einer Formel, sage ψ , dann schreibt man auch $\psi \models \phi$.

Definition 13.6 (Semantische Äquivalenz). Zwei Formeln ϕ und ψ sind semantisch äquivalent, geschrieben $\phi \equiv \psi$, genau dann, wenn $\phi \models \psi$ und $\psi \models \phi$ gilt.

In der Prädikatenlogik können wir nun dieselben Definitionen wie in der Aussagenlogik machen:

Definition 13.7 (Erfüllbarkeit). Eine prädikatenlogische Formel ϕ heißt *erfüllbar*, wenn sie ein Modell hat.

Definition 13.8 (Falsifizierbarkeit). Eine prädikatenlogische Formel ϕ heißt *falsifizierbar*, wenn es ein Modell \mathcal{M} gibt mit $\mathcal{M} \not\models \phi$.

Definition 13.9 (Allgemeingültigkeit). Eine prädikatenlogische Formel ϕ heißt *allgemeingültig*, wenn sie in jedem Modell wahr ist.

Man schreibt dann $\models \phi$ und nennt ϕ eine *Tautologie*.

Definition 13.10 (Unerfüllbarkeit). Eine prädikatenlogische Formel ϕ heißt *unerfüllbar*, wenn es kein Modell für sie gibt.

Man schreibt dann $\not\models \phi$ und nennt ϕ eine *Kontradiktion*.

Auch in der Prädikatenlogik gilt das Dualitätsprinzip:

Satz 13.1 (Dualitätsprinzip). Eine prädikatenlogische Formel ϕ ist genau dann allgemeingültig, wenn $\neg\phi$ unerfüllbar ist.

13.3 Fundamentale Äquivalenzen der Prädikatenlogik

Satz 13.2. ϕ , ψ und χ seien Formeln der Prädikatenlogik, wobei in χ die Variable x nicht vorkommt.

Es gelten folgende (semantische) Äquivalenzen:

$$\begin{aligned}
 \neg(\forall x \phi) &\equiv \exists x (\neg\phi) \\
 \neg(\exists x \phi) &\equiv \forall x (\neg\phi) \\
 \forall x \phi \wedge \forall x \psi &\equiv \forall x (\phi \wedge \psi) \\
 \exists x \phi \vee \exists x \psi &\equiv \exists x (\phi \vee \psi) \\
 \forall x (\forall y \phi) &\equiv \forall y (\forall x \phi) \\
 \exists x (\exists y \phi) &\equiv \exists y (\exists x \phi) \\
 (\forall x \phi) \wedge \chi &\equiv \forall x (\phi \wedge \chi) \\
 (\forall x \phi) \vee \chi &\equiv \forall x (\phi \vee \chi) \\
 (\exists x \phi) \wedge \chi &\equiv \exists x (\phi \wedge \chi) \\
 (\exists x \phi) \vee \chi &\equiv \exists x (\phi \vee \chi)
 \end{aligned}$$

Kapitel 14

Natürliches Schließen in der Prädikatenlogik

In Kapitel 5 wurde das Beweissystems des natürlichen Schließens nach Gerhard Gentzen für die Aussagenlogik eingeführt. Es beruht auf Regeln, wie Formeln (syntaktisch) umgeformt werden dürfen, um aus gegebenen Aussagen Schlussfolgerungen herzuleiten.

Ein wichtiges Ergebnis war dabei die Vollständigkeit des natürlichen Schließens als Beweissystem für die Aussagenlogik, d.h. dass für eine Menge Γ von gegebenen Formeln und eine Formel ϕ der Aussagenlogik gilt:

$$\Gamma \vdash \phi \Leftrightarrow \Gamma \vDash \phi$$

Die „syntaktische Sicht“ und die „semantische Sicht“ sind also äquivalent und wir können zwischen ihnen wechseln, je nachdem welche für eine konkrete Fragestellung besser geeignet ist.

Das Beweissystem des natürlichen Schließens hat Gerhard Gentzen für die Prädikatenlogik (mit Gleichheit) eingeführt. In diesem Kapitel werden die Regeln für die Quantoren und die Gleichheit vorgestellt.

Der Satz über die Vollständigkeit des natürlichen Schließens gilt auch für die Prädikatenlogik. Dies wurde zuerst von Kurt Gödel¹ für das Hilbert-Kalkül gezeigt. Gerhard Gentzen hat ihn für sein Beweissystem des Sequenzkalküls bewiesen. Man muss den Vollständigkeitssatz so begreifen, dass er nicht für ein spezielles Beweissystem gilt, sondern eine Eigenschaft der Logik selbst ist, vorausgesetzt natürlich, dass das Beweissystem „vernünftig“ definiert ist.

¹Kurt Gödel (1906–1978), österreichisch-amerikanischer Logiker.

14.1 Schlussregeln

14.1.1 Allquantor

	<i>Einführung</i>	<i>Elimination</i>
\forall	$\frac{x_0 \quad \vdots \quad \phi[x_0/x]}{\forall x\phi} \quad \forall x i$	$\frac{\forall x\phi}{\phi[t/x]} \quad \forall x e$

Um den Allquantor einzuführen, hat man folgende Beweisverpflichtung: Gegeben sei ein beliebiges Objekt x_0 des Universums. Man muss dann zeigen, dass die Formel ϕ mit x_0 an Stelle der Variablen x gilt (dies schreibt man kurz als $\phi[x_0/x]$). Dabei darf in dieser Herleitung keinerlei *spezielle* Eigenschaft von x_0 vorkommen, denn x_0 steht ja für ein *beliebiges* Objekt des Universums. Man sagt auch, dass x_0 ein *frisches* beliebiges Objekt ist, sein Name darf somit nicht außerhalb der Box vorkommen.

Die Entfernung des Allquantors ist ein naheliegender Schritt: Wenn ϕ für alle x gilt, dann kann man ein beliebiges konkretes t des Universums an Stelle von x in die Formel ϕ einsetzen.

14.1.2 Existenzquantor

	<i>Einführung</i>	<i>Elimination</i>
\exists	$\frac{\phi[t/x]}{\exists x\phi} \quad \exists x i$	$\frac{\exists x\phi}{\frac{x_0 \quad \phi[x_0/x] \quad \vdots \quad \chi}{\chi}} \quad \exists x e$

Den Existenzquantor kann man einführen, indem man einen *Zeugen* vorweist: Gilt ϕ mit t an Stelle von x , dann gibt es offenbar ein x für das ϕ gilt, nämlich eben t .

Will man den Existenzquantor entfernen, muss man ein Objekt x_0 nehmen, das ϕ an Stelle von x erfüllt. Solch ein Objekt existiert, weil ja $\exists x\phi$ gilt. Nun hat man die Beweisverpflichtung zu zeigen, dass daraus χ herleitbar ist. In dieser Herleitung darf man keine spezielle Aussage über x_0 verwenden, außer $\phi[x_0/x]$.

14.1.3 Gleichheit

	<i>Einführung</i>	<i>Elimination</i>
=	$\frac{}{t = t}$ = i, ID	$t_1 = t_2 \quad \phi[t_1/x] \quad \phi[t_2/x]$ = e, SUB

Die Regel ID besagt, dass ein Symbol, das für ein Objekt steht, dieses eindeutig bestimmt. Dies ist gewissermaßen die Charakteristik der Gleichheit.

Die Entfernung der Gleichheit besteht darin, dass wenn t_1 und t_2 gleich sind, man in einer Formel ϕ t_1 durch t_2 ersetzen kann. Dies klingt wie selbstverständlich, muss aber mit Vorsicht gehandhabt werden. Es sind nur gültige Substitutionen erlaubt: In allen Substitutionen $\phi[t/x]$ muss t frei für x in der Formel ϕ sein, d.h. keine freie Variable y in t gelangt durch das Einsetzen von x in ϕ in den Bereich eines Quantors $\forall y$ oder $\exists y$.

14.2 Beispiele

Gentzen zeigt in [Gen35, S. 183] an drei Beispielen, wie das natürliche Schließen geht. Das erste Beispiel für eine Formel der Aussagenlogik wurde in Abschnitt 5.2 verwendet.

Für die Prädikatenlogik verwendet Gentzen die beiden folgenden Beispiele:

Beispiel: Vertauschen von Quantoren

Herleitung für

$$\exists x \forall y F(x, y) \rightarrow \forall y \exists x F(x, y)$$

1.	$\exists x \forall y F(x, y)$	angenommen
2.	a	angenommen
3.	$\forall y F(a, y)$	angenommen
4.	b	beliebig
5.	$F(a, b)$	$\forall e 3, 4$
6.	$\exists x F(x, b)$	$\exists i 2, 5$
7.	$\forall y \exists x F(x, y)$	$\forall i 4-6$
8.	$\forall y \exists x F(x, y)$	$\exists e 1, 2-7$
9.	$\exists x \forall y F(x, y) \rightarrow \forall y \exists x F(x, y)$	$\rightarrow i 1-8$

Negation und Quantoren

Als weiteres Beispiel folgt ein Beweis für

$$\neg \exists x G(x) \rightarrow \forall y \neg G(y)$$

Der Beweis folgt wieder der Argumentation von Gentzen in [Gen35, S. 183]:

1.	$\neg \exists x G(x)$	angenommen
2.	a	beliebig
3.	$G(a)$	angenommen
4.	$\exists x G(x)$	$\exists i 2, 3$
5.	\perp	$\neg e 1, 4$
6.	$\neg G(a)$	$\neg i 3-5$
7.	$\forall y \neg G(y)$	$\forall i 2-6$
8.	$\neg \exists x G(x) \rightarrow \forall y \neg G(y)$	$\rightarrow i 1-7$

14.3 Vollständigkeit des natürlichen Schließens

siehe Vorlesung

Kapitel 15

Unentscheidbarkeit der Prädikatenlogik

siehe Vorlesung

Kapitel 16

Anwendungen der Prädikatenlogik in der Softwaretechnik

siehe Vorlesung

16.1 Analyse von Softwaremodellen mit Alloy

Teil III

Lineare Temporale Logik

Kapitel 17

Dynamische Modelle

siehe Vorlesung

Kapitel 18

Die formale Sprache der linearen temporalen Logik (LTL)

In der Sprache der linearen temporalen Logik (LTL) erweitert man die formale Sprache der Aussagenlogik durch weitere Junktoren, mit denen temporale Eigenschaften formuliert werden können.

Definition 18.1 (Alphabet der LTL). Das *Alphabet* der Sprache der linearen temporalen Logik (LTL) besteht aus

- (i) einer Menge \mathcal{P} von Aussagensymbolen,
- (ii) den (aussagenlogischen) Junktoren: $\neg, \wedge, \vee, \rightarrow$
- (iii) den (temporalen) Junktoren: \circ, \mathcal{U}
- (iv) der Konstanten: \perp
- (v) den zusätzlichen Symbolen: $(,)$

Bemerkungen

- Wie im Falle der Aussagenlogik, definieren wir *eine* Sprache der linearen temporalen Logik durch die Vorgabe der Menge \mathcal{P} und der eben definierten Junktoren.
- Die formale Sprache der LTL ist eine Erweiterung der Aussagenlogik, in der zwei neue Junktoren vorkommen:
 - \circ steht für „zum nächsten Zeitpunkt“ (*next*)
 - \mathcal{U} steht für „bis“ (*until*)

Definition 18.2 (Formeln der LTL). Die *Formeln* der linearen temporalen Logik sind Zeichenketten, die nach folgenden Regeln gebildet werden:

- (i) Jedes Symbol $P \in \mathcal{P}$ ist eine Formel und auch \perp ist eine Formel.
- (ii) Ist ϕ eine Formel, dann auch $\neg\phi$.
- (iii) Sind ϕ und ψ Formeln, dann auch $(\phi \wedge \psi)$, $(\phi \vee \psi)$ und $(\phi \rightarrow \psi)$
- (iv) Ist ϕ eine Formel, dann auch $\circ\phi$.
- (v) Sind ϕ und ψ Formeln, dann auch $(\phi \mathcal{U} \psi)$

Als *Grammatik* in Backus-Naur-Darstellung können wir diese induktive Definition der Formeln der LTL so ausdrücken:

$$\phi ::= P \mid \perp \mid \neg\phi \mid (\phi \wedge \phi) \mid (\phi \vee \phi) \mid (\phi \rightarrow \phi) \mid \circ \phi \mid (\phi \mathcal{U} \phi)$$

mit Variablen $P \in \mathcal{P}$ und (bereits gebildeten) Formeln ϕ .

Die Präzedenz der Junktoren wird folgendermaßen definiert: Die unären Junktoren \neg und \circ binden stärker als die binären, sie selbst binden gleich stark. Binäre Junktoren binden in folgender Reihenfolge, die stärkste Bindung zuerst: $\mathcal{U}, \wedge, \vee, \rightarrow$. Außerdem sind \wedge und \vee linksassoziativ, \mathcal{U} und \rightarrow sind rechtsassoziativ.

Bemerkung

In Formeln der LTL werden wir oft vier weitere Junktoren verwenden, die folgendermaßen definiert werden:

$$\begin{aligned}\diamond \phi &\stackrel{\text{def}}{=} \neg \perp \mathcal{U} \phi \\ \Box \phi &\stackrel{\text{def}}{=} \neg \diamond \neg \phi \\ \phi \mathcal{W} \psi &\stackrel{\text{def}}{=} (\phi \mathcal{U} \psi) \vee \Box \phi \\ \phi \mathcal{R} \psi &\stackrel{\text{def}}{=} \neg (\neg \phi \mathcal{U} \neg \psi)\end{aligned}$$

Wir lesen sie so:

- \diamond steht für „irgendwann“ (*eventually*),
- \Box steht für „immer“ (*always*),
- \mathcal{W} steht für „sofern nicht“ (*unless, weak until*) und
- \mathcal{R} steht für „löst ab“ (*release*).

\diamond und \Box haben dieselbe Bindungspräzedenz wie \circ und \mathcal{W} und \mathcal{R} die von \mathcal{U} .

Kapitel 19

Die Semantik der linearen temporalen Logik (LTL)

19.1 Kripke-Struktur

Modelle in der temporalen Logik enthalten ein implizites Konzept einer diskreten Zeit: Man denkt sich die „Welt“ des Modells als bestehend aus Zuständen, in denen gewissen Aussagen wahr sind und einer Übergangsrelation der Zustände. Jeder Zustandsübergang entspricht dann gerade einem Zeitschritt. Präziser definiert man die Kripke-Struktur¹:

Definition 19.1 (Kripke-Struktur). Eine *Kripke-Struktur* \mathcal{K} ist ein Tupel (S, s_0, \rightarrow, L) bestehend aus

- einer Menge von Zuständen S ,
- einem ausgezeichneten Startzustand $s_0 \in S$,
- einer Übergangsrelation $\rightarrow \subseteq S \times S$, die jedem Zustand s einen Folgezustand s' zuordnet (d.h. $\forall s \exists s' \text{ mit } s \rightarrow s'$) und
- einer Beschriftungsfunktion $L : S \rightarrow \mathbb{P}(\mathcal{P})$ von S in die Potenzmenge von \mathcal{P} , die jedem Zustand eine Menge von (wahren) Aussagenatomen zuordnet.

Bemerkungen

1. Man könnte in die Definition der Kripke-Struktur auch die Wahl von \mathcal{P} explizit aufnehmen. In den Beispielen, die wir betrachten, ergibt sich die Menge der Atome aus der Beschriftungsfunktion.
2. Die Beschriftungsfunktion L ordnet jedem Zustand die in diesem Zustand wahren Aussagen aus \mathcal{P} zu. Dies kann man auch so sehen: L ordnet jedem Zustand s eine Belegung $v_s : \mathcal{P} \rightarrow \mathbb{B}$ zu.

¹Saul A. Kripke (* 1940), amerikanischer Logiker.

3. Eine Kripke-Struktur kann man als gerichteten Graphen sehen, in dem die Zustände S die Knoten sind und die Übergangsrelation gerade die gerichteten Kanten. Zudem wird jeder Zustand mit den in ihm gültigen Aussagen gemäß der Beschriftungsfunktion L markiert. Der Startzustand wird durch einen eingehenden Pfeil ohne Startknoten markiert.
4. Manchmal zeichnet man in einer Kripke-Struktur keinen Startzustand aus, man bezeichnet sie dann als Übergangssystem (siehe [HR04, Abschnitt 3.2]).
5. Manche Autoren lassen in Kripke-Strukturen auch mehrere Startzustände zu.
6. Wenn in einem konkreten System die Übergangsrelation nicht die Eigenschaft hat, dass es zu jedem Zustand einen Folgezustand gibt, kann man den Graph um einen Zustand erweitern, der einen Übergang auf sich selbst hat und hat damit die Definition einer Kripke-Struktur erfüllt.

Beispiele In Abb. 19.1 und 19.2 werden die Graphen zu zwei Beispielen dargestellt.

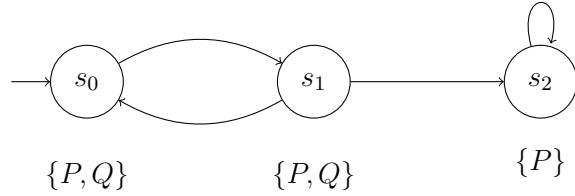


Abbildung 19.1: Beispiel einer Kripke-Struktur

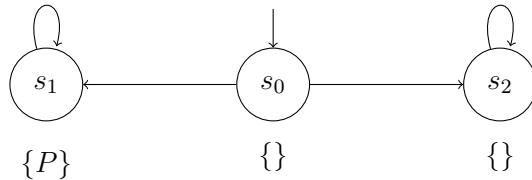


Abbildung 19.2: Beispiel für die Semantik der Negation

Definition 19.2 (Pfad und Berechnung). Sei $\mathcal{K} = (S, s_0, \rightarrow, L)$ eine Kripke-Struktur.

Ein *Pfad* π ist eine unendliche Folge s_1, s_2, s_3, \dots von Zuständen $s_i \in S$ mit $s_i \rightarrow s_{i+1}$ für alle $i \geq 1$. Man schreibt einen Pfad gerne so:

$$\pi = s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$$

Hat man einen Pfad $\pi = s_1 \rightarrow s_2 \rightarrow s_3 \dots$ gegeben, dann bezeichnet man mit π^i den Pfad, der im i -ten Zustand von π beginnt, also z.B. $\pi^2 = s_2 \rightarrow s_3 \rightarrow s_4 \dots$

Eine *Berechnung* ist ein Pfad, der mit dem Startzustand $s_0 \in S$ beginnt.

Nun haben wir alle Notation, um Semantiken der LTL definieren zu können:

Definition 19.3 (Semantik der LTL für einen Pfad). Sei \mathcal{K} eine Kripke-Struktur und $\pi = s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$ ein Pfad. Für eine Formel ϕ der linearen temporalen Logik definiert man

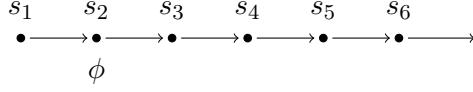
$$\pi \models \phi,$$

falls $\llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = T$. Dabei wird $\llbracket \phi \rrbracket_{\pi}^{\mathcal{K}}$ induktiv definiert über den strukturellen Aufbau von ϕ

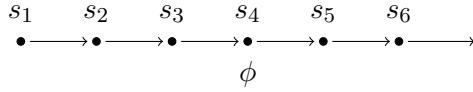
- (i) $\llbracket \perp \rrbracket_{\pi}^{\mathcal{K}} := F$
- (ii) $\llbracket P \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } P \in L(s_1) \\ F & \text{sonst} \end{cases}$
- (iii) $\llbracket \neg \phi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = F \\ F & \text{sonst} \end{cases}$
- (iv) $\llbracket \phi \wedge \psi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = T \text{ und } \llbracket \psi \rrbracket_{\pi}^{\mathcal{K}} = T \\ F & \text{sonst} \end{cases}$
- (v) $\llbracket \phi \vee \psi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = T \text{ oder } \llbracket \psi \rrbracket_{\pi}^{\mathcal{K}} = T \\ F & \text{sonst} \end{cases}$
- (vi) $\llbracket \phi \rightarrow \psi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = F \text{ oder } \llbracket \psi \rrbracket_{\pi}^{\mathcal{K}} = T \\ F & \text{sonst} \end{cases}$
- (vii) $\llbracket \circ \phi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \llbracket \phi \rrbracket_{\pi^2}^{\mathcal{K}} = T \\ F & \text{sonst} \end{cases}$
- (viii) $\llbracket \phi \mathcal{U} \psi \rrbracket_{\pi}^{\mathcal{K}} := \begin{cases} T & \text{falls } \exists i \geq 1 \text{ mit } \llbracket \psi \rrbracket_{\pi^i}^{\mathcal{K}} = T \\ & \text{und } \forall j=1, \dots, i-1 \llbracket \phi \rrbracket_{\pi^j}^{\mathcal{K}} = T \\ F & \text{sonst} \end{cases}$

Veranschaulichung der Semantik der temporalen Operatoren der LTL

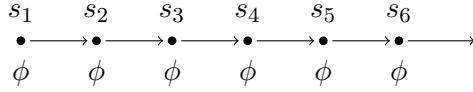
- $\circ\phi$ bedeutet, dass ϕ im nächsten Zustand gilt:



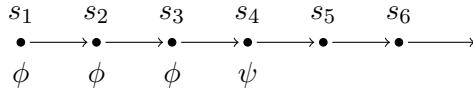
- $\Diamond\phi$ bedeutet, dass ϕ irgendwann auf dem Pfad gilt:



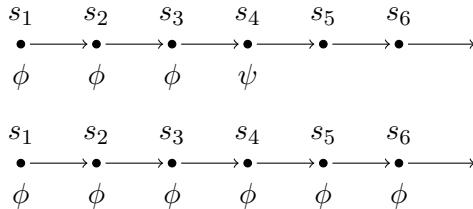
- $\Box\phi$ bedeutet, dass ϕ immer auf dem Pfad gilt:



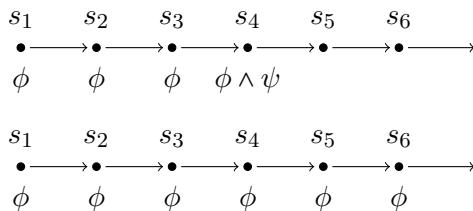
- $\phi\mathcal{U}\psi$ bedeutet, dass ψ irgendwann auf dem Pfad gilt, und dass bis dahin auf jeden Fall ϕ wahr ist:



- $\phi\mathcal{W}\psi$ bedeutet, dass ϕ gilt bis ψ gilt oder für immer, wenn ein solcher Zustand nicht existiert:



- $\phi\mathcal{R}\psi$ bedeutet, dass ϕ gilt einschließlich dem ersten Zustand, in dem ψ gilt oder immer, wenn ein solcher Zustand nicht existiert:



Definition 19.4 (Semantik für Pfade, Zustände und Strukturen). Sei \mathcal{K} eine Kripke-Struktur. Es gilt dann

- Sei π ein *Pfad* über \mathcal{K} . Dann sagt man, dass π eine Formel ϕ erfüllt, geschrieben $\pi \models \phi$, wenn gilt $\llbracket \phi \rrbracket_{\pi}^{\mathcal{K}} = \top$.
- Sei s ein *Zustand* von \mathcal{K} . Dann sagt man, dass s eine Formel ϕ erfüllt, geschrieben $s \models \phi$, wenn für alle Pfade π , die mit s beginnen, gilt $\pi \models \phi$.
- Man sagt, dass die *Kripke-Struktur* \mathcal{K} eine Formel ϕ erfüllt, geschrieben $\mathcal{K} \models \phi$, wenn für den Startzustand s_0 gilt: $s_0 \models \phi$.

Beispiele Wenn wir zunächst das obige Beispiel 19.1 betrachten, ist leicht zu sehen, dass gilt:

- $\mathcal{K} \models \Box P$
denn in allen Zuständen ist P true.
- $s_0 \models \Diamond(P \vee Q)$
denn in s_1 gilt $P \vee Q$.
- $s_0 \models \Diamond(P \wedge Q)$
denn in s_1 gilt $P \wedge Q$.
- $s_1 \not\models \Diamond(P \wedge Q)$
denn zwar gilt in s_0 gilt $P \wedge Q$, nicht aber in s_2 .
- $\mathcal{K} \models \Box(\neg Q \rightarrow \Box(P \wedge \neg Q))$
denn der einzige Zustand mit $\neg Q$ ist s_2 , ab dann gilt aber immer $P \wedge \neg Q$.

An Beispiel 19.2 kann man sehen, dass obgleich für Pfade gilt $\pi \models \phi \Leftrightarrow \pi \not\models \neg\phi$ gilt, dies für Kripke-Strukturen nicht der Fall ist:

- $\mathcal{K} \not\models \Diamond P$
denn auf dem Pfad $s_0 \rightarrow s_2 \rightarrow s_2 \rightarrow \dots$ ist P niemals true.
- $\mathcal{K} \not\models \neg\Diamond P$
denn auf dem Pfad $s_0 \rightarrow s_1 \rightarrow s_1 \rightarrow \dots$ ist P schließlich true.

Bemerkung Die Semantik der linearen temporalen Logik unterscheidet sich grundlegend je nach Definition. Betrachtet man die Semantik der LTL für Pfade, dann gilt der Satz vom ausgeschlossenen Dritten, d.h. $\models_{\pi} \phi \vee \neg\phi$ für eine beliebige Formel ϕ der LTL. Für die Semantik der LTL für Kripke-Strukturen ist dies nicht der Fall. Obiges Beispiel zeigt, dass es Kripke-Strukturen geben kann, in denen weder ϕ noch $\neg\phi$ gilt. Das liegt daran, dass es in einer Kripke-Struktur Pfade π_1 und π_2 geben kann, für die $\pi_1 \models \phi$ und $\pi_2 \models \neg\phi$ gilt.²

²Dass der Satz vom ausgeschlossenen Dritten (*Tertium non datur*) *nicht* richtig ist, gilt auch für die Kripke-Semantik der intuitionistischen Logik. Diese Semantik

Für die Definition von Erfüllbarkeit, Allgemeingültigkeit und semantischer Äquivalenz wird die Pfad-Semantik zugrundegelegt.

Definition 19.5 (Erfüllbarkeit, Allgemeingültigkeit).

- Eine Formel ϕ heißt *erfüllbar*, wenn es eine Kripke-Struktur gibt mit einem Pfad π so dass gilt $\pi \models \phi$.
- Eine Formel ϕ heißt *allgemeingültig*, wenn für alle Pfade in allen Kripke-Strukturen gilt: $\pi \models \phi$.

Definition 19.6 (Semantische Äquivalenz). Zwei Formeln ϕ und ψ sind *semantisch äquivalent*, geschrieben $\phi \equiv \psi$, wenn für alle Pfade π gilt: $\pi \models \phi \Leftrightarrow \pi \models \psi$.

19.2 Äquivalenzen von Formeln der LTL

- Dualität

$$\begin{aligned}\neg \circ \phi &\equiv \circ \neg \phi \\ \neg \diamond \phi &\equiv \square \neg \phi \\ \neg \square \phi &\equiv \diamond \neg \phi\end{aligned}$$

- Idempotenz

$$\begin{aligned}\diamond \diamond \phi &\equiv \diamond \phi \\ \square \square \phi &\equiv \square \phi \\ \phi \mathcal{U} (\phi \mathcal{U} \psi) &\equiv \phi \mathcal{U} \psi \\ (\phi \mathcal{U} \psi) \mathcal{U} \psi &\equiv \phi \mathcal{U} \psi\end{aligned}$$

- Absorption

$$\begin{aligned}\diamond \square \diamond \phi &\equiv \square \diamond \phi \\ \square \diamond \square \phi &\equiv \diamond \square \phi\end{aligned}$$

wird über Kripke-Strukturen definiert, die zusätzlich zu unserer Definition die Eigenschaft der *Monotonie* haben. Diese Eigenschaft bedeutet, dass in jedem Folgezustand s' eines beliebigen Zustands s gilt: $L(s) \subseteq L(s')$. D.h. also, dass mit jedem Zustandsübergang mehr atomare Aussagen wahr werden.

Die Semantik der Junktoren der intuitionistischen Aussagenlogik werden dann in den Begriffen der LTL so definiert:

- $P \wedge Q \stackrel{\text{def}}{=} \mathcal{K} \models P \wedge Q$
- $P \vee Q \stackrel{\text{def}}{=} \mathcal{K} \models P \vee Q$
- $\neg P \stackrel{\text{def}}{=} \mathcal{K} \models \neg \diamond P$
- $P \rightarrow Q \stackrel{\text{def}}{=} \mathcal{K} \models \square(P \rightarrow Q)$

Siehe [Bor05, Chap. 9] sowie [vD13, Section 6.3].

- Expansion

$$\phi \mathcal{U} \psi \equiv \psi \vee (\phi \wedge \circ(\phi \mathcal{U} \psi))$$

$$\diamond \phi \equiv \phi \vee \circ \diamond \phi$$

$$\square \phi \equiv \phi \wedge \circ \square \phi$$

- Distributiv-Gesetze

$$\diamond (\phi \vee \psi) \equiv \diamond \phi \vee \diamond \psi$$

$$\square (\phi \wedge \psi) \equiv \square \phi \wedge \square \psi$$

$$\circ (\phi \mathcal{U} \psi) \equiv \circ \phi \mathcal{U} \circ \psi$$

19.3 Typische Aussagen in der LTL

siehe Vorlesung

Kapitel 20

Natürliches Schließen in der LTL

siehe Vorlesung

Kapitel 21

Anwendungen der LTL in der Softwaretechnik

siehe Vorlesung

21.1 Model Checking

21.1.1 Konzept des Model Checkings

21.1.2 Der Model Checker **SPIN**

21.1.3 Beispiele für Model Checking

21.2 Zielemodell in der Anforderungsanalyse

Literaturverzeichnis

- [ABKS13] SVEN APEL, DON BATORY, CHRISTIAN KÄSTNER, ET AL. *Feature-Oriented Software Product Lines*. Berlin Heidelberg: Springer, 2013.
- [Bat05] DON S. BATORY. Feature Models, Grammars, and Propositional Formulas. In: *Software Product Lines, 9th International Conference, SPLC 2005, Rennes, France, September 26–29, 2005, Proceedings, Lecture Notes in Computer Science*, Band 3714, S. 7–20. Springer, 2005.
- [Bor05] RICHARD BORNAT. *Proof and Disproof in Formal Logic: An introduction for programmers*. Oxford: Oxford University Press, 2005.
- [BR18] DANIEL LE BERRE, PASCAL RAPICAULT. Boolean-Based Dependency Management for the Eclipse Ecosystem. *International Journal on Artificial Intelligence Tools*, 27(1):1–23, 2018.
- [DLL62] MARTIN DAVIS, GEORGE LOGEMANN, DONALD LOVELAND. A machine program for theorem-proving. *Commun. ACM*, 5(7):394–397, 1962.
- [dMB10] LEONARDO MENDONÇA DE MOURA, NIKOLAJ BJØRNER. Applications and Challenges in Satisfiability Modulo Theories. In: *Second International Workshop on Invariant Generation, WING 2009, York, UK, March 29, 2009 and Third International Workshop on Invariant Generation, WING 2010, Edinburgh, UK, July 21, 2010, EPiC Series in Computing*, Band 1, S. 1–11. 2010.
- [DP60] MARTIN DAVIS, HILARY PUTNAM. A Computing Procedure for Quantification Theory. *J. ACM*, 7(3):201–215, 1960.
- [GBE⁺14] JÜRGEN GIESL, MARC BROCKSCHMIDT, FABIAN EMMES, ET AL. Proving Termination of Programs Automatically with AProVE. In: *Automated Reasoning - 7th International Joint*

- Conference, IJCAR 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 19–22, 2014. Proceedings, Lecture Notes in Computer Science*, Band 8562, S. 184–191. Springer, 2014.
- [Gen35] GERHARD GENTZEN. Untersuchungen über das logische Schließen. I. *Mathematische Zeitschrift*, 39:176–210, 1935. URL <http://gdz.sub.uni-goettingen.de/dms-resolveppn/?PPN=GDZPPN002375508>.
 - [Hed04] SHAWN HEDMAN. *A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity*. Oxford: Oxford University Press, 2004.
 - [Hof11] DIRK W. HOFFMANN. *Grenzen der Mathematik: Eine Reise durch die Kerngebiete der mathematischen Logik*. Heidelberg: Spektrum Akademischer Verlag, 2011.
 - [HR04] MICHAEL HUTH, MARK RYAN. *Logic in Computer Science: Modelling and Reasoning about Systems*. Cambridge, UK: Cambridge University Press, 2. Auflage, 2004.
 - [KCH⁺90] KYO C. KANG, SHOLOM G. COHEN, JAMES A. HESS, ET AL. *Technical Report: Feature-Oriented Domain Analysis (FODA) Feasability Study*. Pittsburgh, PA: Software Engineering Institute (SEI), 1990.
 - [KGN⁺09] ROOPE KAIVOLA, RAJNISH GHUGHAL, NAREN NARASIMHAN, ET AL. Replacing Testing with Formal Verification in Intel Core i7 Processor Execution Engine Validation. In: *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings, Lecture Notes in Computer Science*, Band 5643, S. 414–429. Springer, 2009.
 - [Knu15] DONALD E. KNUTH. *The Art of Computer Programming, Volume 4, Fascicle 6: Satisfiability*. Boston, MA: Addison-Wesley, 2015.
 - [KS06] DANIEL KROENING, OFER STRICHMAN. *Decision Procedures: An Algorithmic Point of View*. Springer, 2006.
 - [MH07] ANDREAS METZGER, PATRICK HEYMANS. *Technischer Bericht: Comparing Feature Diagram Examples Found in the Research Literature*. Software Systems Engineering, Universität Duisburg-Essen, 2007.
 - [MTS⁺17] JENS MEINICKE, THOMAS THÜM, REIMAR SCHRÖTER, ET AL. *Mastering Software Variability with FeatureIDE*. Springer, 2017.

- [Rau08] WOLFGANG RAUTENBERG. *Einführung in die Mathematische Logik, 3., überarbeitete Auflage*. Vieweg + Teubner, 2008.
- [SKK03] CARSTEN SINZ, ANDREAS KAISER, WOLFGANG KÜCHLIN. Formal methods for the validation of automotive product configuration data. *AI EDAM*, 17(1):75–97, 2003.
- [Tse83] G. S. TSEITIN. On the Complexity of Derivation in Propositional Calculus. In: J. SIEKMANN, G. WRIGHTSON, Hg., *Automation of Reasoning 2: Classical Papers on Computational Logic 1967-1970*, S. 466–483. Berlin, Heidelberg: Springer, 1983.
- [vD13] DIRK VAN DALEN. *Logic and Structure*. Berlin: Springer, 5. Auflage, 2013.