Einführung in die Computationelle Logik

Christian Wurm
cwurm@phil.hhu.de

January 29, 2024

Contents

1 Was ist Logik? 4

2 Aussagenlogik – Syntax 6

3 Aussagenlogik – Semantik 8

4 Aussagenlogik - Semantik II 10

5 Tautologien, Widersprüche etc. 14

6 Entscheidbarkeit 16

7 Interdefinierbarkeit und funkionale Vollständigkeit 17
7.1 Interdefinierbarkeit 17
7.2 Funktionale Vollständigkeit 19

8 Tableau Methoden und Entscheidbarkeit 23

9 Noch eine Semantik: Boolesche Algebren 29
9.1 Strukturtheorie 29
9.2 Interpretation von Formeln in Algebren 35

10 Beweistheorie 37
10.1 Allgemeines 37
10.2 Der Kalkül CL 38

10.3 Die “Bedeutung” von Sequenten 40
10.4 Entscheidbarkeit und Schnitt 41

11 Die wichtigsten Ergebnisse in Kürze 46
11.1 Substitutionen 46
11.2 Konsistenz, Maximalkonsistenz 47
11.3 Schnitt-Eliminierung 48
11.4 Vollständigkeit 49

12 Prädikatenlogik – Syntax 51

13 Prädikatenlogik – Semantik 53

14 Wahrheit und Konsequenz in Prädikatenlogik 59
14.1 Die Frage nach der Wahrheit im Modell 59
14.2 Semantische Konsequenz 59

15 Interdefinierbarkeit und wichtige Tautologien 64

16 Beweistheorie der Prädikatenlogik 65

17 Theorien und Modelle, Axiome 69
17.1 Partielle Ordnungen 71
17.2 Lineare Ordnungen 73
17.3 Endlichkeit und Wohlordnung (Exkurs) 77
17.4 Bäume 78
17.5 Hausaufgabe zum 17.1.2022 81

18 Definierbarkeit von Prädikaten und die Bedeutung von offenen Formeln in Theorien 82
18.1 Analysis und Körper 87

19 Peano Arithmetik 89

20 Definierbarkeit und die Bedeutung von offenen Formeln 92

21 Normalformen 99
21.1 Prenex Normalform 99
21.2 Die arithmetische Hierarchie 103

22 Entscheidbarkeit **104**
22.1 Einleitung: Turing Maschinen 104
22.2 Unentscheidbarkeit 106
22.3 Was hat das mit Prädikatenlogik zu tun? 109
22.4 Entscheidbarkeit 111

23 Fragmente **111**

24 Entscheidbare Theorien **112**

25 Zusammenfassung **112**

1 Was ist Logik?

Es ist schwierig, das zu sagen, ohne auf der anderen Seite falsche Vorurteile zu sähen oder mit abstrakten mathematischen Definitionen Unverständnis zu ernten. Ziel der Logik ist es, ganz allgemein ausgedrückt, ein mathematisches Modell für das zu konstruieren, was wir intuitiv logisches Denken nennen. Wir wollen also eine Sprache, die für uns klar macht, welche Argumente und Schlüsse **valide**, als allgemein gültig sind, und welche nicht. Das besondere an der Logik ist, dass wir diese Unterscheidung treffen wollen nur anhand der **syntaktischen Form**: wir schauen uns also einen logischen Satz an, und nur anhand seiner Form sehen wir (z.B.), ob er eine allgemeine Wahrheit ausdrückt oder nicht. Z.B. der Satz

(1) Es regnet oder es regnet nicht.

scheint allgemein wahr zu sein, und um das zu sagen, müssen wir nicht wissen was regen ist – es reicht die syntaktische Form. Was in natürlichen Sprachen in Ausnahmefällen geht, soll in der Logik immer gehen: wir suchen eine formale Sprache, bei der wir die Validität ihrer Sätze an der syntaktischen Form ablesen können. In diesem Sinne ist Logik einfach ein Teil der Theorie der formalen Sprachen: wir sind interessiert in Mengen von Sätzen:

1. Die wohlgeformten Formeln (also Aussagen, die wahr oder falsch sein können),
2. Die sog. Theoreme, also die Formeln/Sätze, die allgemeine Wahrheiten ausdrücken
3. Die sog. Kontradiktionen, also Sätze, die immer falsch sind
4. ...und einige mehr.

Diese Situation ist allerdings noch unbefriedigend: wenn wir einfach nur in Mengen von Sätzen interessiert sind, bleibt der Begriff der Wahrheit inhaltsleer und beliebig: alles mögliche können wir als wahr und falsch definieren. Um diesen Begriff mit Leben zu füllen, müssen wir unseren logischen Sätzen eine **Bedeutung** geben. Hier ist der zentrale Begriff der eines **Modells**: Modelle sind abstrakte mathematische Strukturen, die aber im Prinzip (stark vereinfachte) Nachbildungen der Wirklichkeit darstellen sollen. Wenn wir ein Modell haben, dann können wir sagen:

(2) Die Formel ϕ ist wahr/falsch im Modell M.

Das sollte man definieren mittels einer **kompositionalen Semantik**: die Wahrheit einer komplexen Formel basiert auf der Wahrheit ihrer Teilformeln, und der Art wie sie zusammengefügt werden. Hiermit lässt sich nun ganz einfach das Problem stellen: sind die Formeln, die (rein syntaktisch) Theoreme sind, genau dieselben, die in allen Modellen wahr sind? Dieses Problem nennt man die Frage der Vollständigkeit, und es ist eines der zentralen Probleme der Logik.

Wir haben also folgende Zutaten der Logik:

1. Eine formale Sprache von Formeln, Theoremen etc.
2. Modelle, die mathematische Strukturen sind und Wahrheit und Falschheit definieren
3. Interpretationen von Formeln in Modelle

Das liefert den Stoff für folgende Fragen:

1. Welche Sprache nutzen wir? Können wir entscheiden ob eine Formel ein Theorem ist, und wie schwer ist das?
2. Welche Modelle sollen wir nutzen, und welche Eigenschaften von Modellen können wir mit unserer Sprache ausdrücken?
3. Wie können wir entscheiden, ob eine Formel in einem Modell wahr ist?
4. Sind unsere Theoreme die Formeln, die wahr sind in allen ihren Modellen?

Damit haben wir schon alle wichtigen Fragen der Logik zusammen. Im Allgemeinen gilt: je expressiver eine Logik, also je mehr wir damit sagen können desto schwieriger wird es, die Frage nach ihrer Wahrheit/Falschheit zu beantworten. Das bedeutet: das ganze Feld lebt von einem *trade-off* Zwischen Expressivität, die wir maximieren möchten, und Komplexität, die wir minimieren möchten. Wir fangen naturgemäß ganz unten an, mit Aussagenlogik.

2 Aussagenlogik – Syntax

Die Syntax der Aussagenlogik ist sehr einfach. Wir haben üblicherweise eine unendliche Menge atomarer Propositionen, z.B.

$$Var = \{p_1, p_2, p_3, ...\}$$

Wir haben weiterhin 4 Konnektoren: $\wedge, \vee, \neg, \rightarrow$. Die **wohlgeformten Formeln** `WFF` sind wie folgt definiert:

1. Falls $p \in Var$, dann ist $p \in$ `WFF`.
2. Falls $\alpha, \beta \in$ `WFF`, dann ist $(\alpha \wedge \beta), (\alpha \vee \beta), (\neg\alpha), (\alpha \rightarrow \beta) \in$ `WFF`.
3. Sonst ist nichts in `WFF`.

`WFF` ist also eine formale Sprache; und die Art, wie wir diese Sprache definieren, nennt man auch eine **induktive Definition**; induktiv, weil wir einen Basisfall haben (1.), dann wohlgeformte Formeln aus wohlgeformten Formeln definieren (2.), und weiterhin sichergehen dass jede Formel auf diese Art konstruiert wird. Diese Art der Definition ist sinnvoll, weil sie es erlaubt, Eigenschaften von Formeln mittels Induktion über deren Komplexität zu beweisen.

Alternativ könnte man auch eine kontextfreie Grammatik schreiben:

- $S \Rightarrow p_1|p_2|p_3|....$
- $S \Rightarrow (S \wedge S)|(S \vee S)|(\neg S)|(S \rightarrow S)$

wobei $p_1, p_2, p_3, ..., \wedge, \vee, \neg, \rightarrow$ die Terminalsymbole sind. Wichtig ist hierbei also: `WFF` ist erstmal eine **formale Sprache**. Allerdings ist es eine formale Sprache, die mit gewissen Intuitionen kommt, nämlich:

- p_1 etc. steht für eine beliebige Proposition, wie z.B. "der Himmel ist blau", oder "das Gras ist rot"
- $\wedge$ korrespondiert mit unserem `und`
- $\vee$ korrespondiert mit unserem `oder`
- $\neg$ korrespondiert mit unserem `nicht`
- $\rightarrow$ korrespondiert mit unserem `wenn...dann...`

Wir können uns also unter aussagenlogischen Formeln komplexe Propositionen vorstellen, die aus einfachen, atomaren Propositionen zusammengefügt werden. Wichtig ist aber: das ist nur eine grobe Intuition, bisher ist `WFF` eine formale Sprache, deren Formeln keinerlei Bedeutung haben.

3 Aussagenlogik – Semantik

Wir haben oben besprochen, dass Formeln wahr oder falsch sind in Modellen. Die Modelle der Aussagelogik sind denkbar einfach. Sie orientieren sich in gewissem Sinne an einem berühmten Diktum von Wittgenstein:

(3) Die Welt ist alles was der Fall ist.

Die Welt ist also die Gesamtheit der wahren Propositionen. Und so einfach ist das: für uns ist eine Gesamtheit (normalerweise) eine Menge, und ein aussagenlogisches Modell ist eine Menge von *atomaren* Propositionen, nämlich die Propositionen, die "der Fall" sind. Ein Modell ist also nichts weiter eine Menge

$$M \subseteq Var$$

Was heißt es nun, dass eine atomare Proposition wahr ist? Sie ist wahr wenn Sie der Fall ist:

$M \models p_i$ genau dann wenn $p_i \in M$.

Das bedeutet also: eine atomare Proposition ist wahr, wenn sie im Modell enthalten, also der Fall ist. Das ist soz. die Grundlage der propositionalen Wahrheit, und hierauf baut der Wahrheitsdefinition komplexer Formeln auf:

$M \models \alpha \wedge \beta$, genau dann wenn $M \models \alpha$ und $M \models \beta$.
$M \models \alpha \vee \beta$, genau dann wenn mindestens eines der beiden gilt, $M \models \alpha$ oder $M \models \beta$.
$M \models \neg\alpha$, gdw. $M \not\models \alpha$
$M \models \alpha \rightarrow \beta$, gdw. mindestens eines der beiden gilt, $M \not\models \alpha$ oder $M \models \beta$.

Hier sind einige Kommentare nötig.

1. Die Definition von $\vee$ gibt das sog. "logische oder", was allgemein soviel heißt wie: mindestens eines der beiden. Man muss das unbedingt unterscheiden vom exklusiven oder, was soviel heißt wie "höchstens eines der beiden". Wenn wir hier "oder" sagen, meinen wir das zukünftig immer im logischen Sinn.

2. $M \not\models p$ bedeutet soviel wie: "$M \models p$ ist falsch"

3. Der logische $\rightarrow$ ist etwas problematisch und wurde bereits viel diskutiert. Man kann auch schreiben: $M \models p \rightarrow q$, gdw. falls $M \models p$, dann gilt auch $M \models q$. Das kann aber leicht zu Missverständnissen führen!

Wir sehen hier also bereits dass große Problem der Logik: sie gibt zwar vor, unsere "natürlichen" Konnektoren "und", "oder" etc. wiederzugeben, aber es ist gar nicht so klar dass sie das wirklich tut! Deswegen ist es wichtig, sich im Zweifelsfall immer an die formalen Definitionen zu halten.

Man sieht bereits aus der Definition, dass

$$p \rightarrow q \text{ gleichbedeutend ist mit } \neg p \vee q.$$

Das ist erstmal gegen unsere Intuition: warum sollte das so sein? Der Sinn dahinter ist folgender: falls $\neg p$ falsch ist, dann ist p wahr, also muss in diesem Fall auch q wahr sein ("wenn p, dann q"). Wenn aber p falsch ist, dann spielt es keine Rolle ob q wahr ist – die sog. Prämissen ist nicht erfüllt, also ist die Konklusion irrelevant. Diese Verwendung des Konditionals widerspricht oft unserer Intuition; wenn aber ein Mathematiker ein Konditional verwendet ("wenn..., dann..."), dann meint er es immer in diesem Sinne. Man nennt diese Tatsache auch: *ex falso quodlibet*, was soviel bedeutet wie: wenn die Prämisse falsch ist, ist das Konditional immer wahr, frei übersetzt: aus einer falschen Prämisse kann man beliebige Folgerungen ziehen.

Übung 1

Bearbeiten bis zum 9.11.2020. Bitte das Video vorher betrachten!

Sei $M = \{p_1, p_3, p_4\}$. Stimmen folgende Aussagen?

1. $M \models (p_1 \vee p_2) \rightarrow p_5$
2. $M \models (\neg(p_1 \wedge p_2)) \vee p_5$
3. $M \models \neg((p_1 \rightarrow p_2) \wedge p_4)$

4 Aussagenlogik - Semantik II

Für unsere Semantik kann man folgende Beobachtung machen:

Satz 1 *Ob $M \models \alpha$ oder $M \not\models \alpha$ hängt nur von denjenigen $p \in Var$ ab, die in α überhaupt vorkommen.*

Z.B. gilt also:

$M \models (p_1 \wedge \neg p_2) \rightarrow p_3$ genau dann wenn $M \cap \{p_1, p_2, p_3\} \models (p_1 \wedge \neg p_2) \rightarrow p_3$.

Das bedeutet, in Bezug auf eine gewisse Formel interessiert uns nur, was ein Modell über deren Teilformeln sagt. Wie beweist man so eine (recht offensichtliche) Behauptung wie Satz 1? Hieran kann man sehr schön die Methode der **Induktion über Formelkomplexität** illustrieren:

- (Induktionsbasis) Die Aussage gilt offensichtlich für alle Formeln der Form $p : p \in Var$, per Definition, da $M \models p$ gdw. $p \in M$ gdw. $p \in M \cap \{p\}$.
- (Induktionshypothese) Nimm an, es gilt für alle Formeln α, β mit Länge $\leq n$, für ein beliebiges n.
- Da die Wahrheit von $\alpha \wedge \beta$ alleine abhängt von der Wahrheit von α und β und *sonst nichts* (qua Definition), gilt die Behauptung auch für $\alpha \wedge \beta$.
- Dasselbe Argument gilt ebenso für $\alpha \vee \beta$, $\neg\alpha$, $\alpha \rightarrow \beta$.
- Also gilt es für alle Formeln der Länge $n+1$, da alle diese Formeln eine der obengenannten Formen haben.
- Also gilt es für **alle Formeln**, da Formeln induktiv definiert sind!

Die induktive Definition erlaubt uns also induktive Beweise. Was wir hier an der Arbeit sehen ist ein wichtiges Prinzip der klassischen Logik, nämlich dass der **Wahrheitsfunktionalität**.

Prinzip der Wahrheitsfunktionalität, schwach Die Wahrheit einer (nicht-atomaren) Formel ist eine Funktion der Wahrheitswerte ihrer unmittelbaren Teilformeln (also z.B. $\alpha \wedge \beta$ hängt von α, β ab).

In der Logik bezeichnet man üblicherweise

- Wahrheit mit "1",
- Falschheit mit "0".

Das ist nur eine Konvention, macht aber vieles einfacher. Beispielsweise können wir nun unsere binären logischen Konnektoren einfach als Funktionen schreiben, z.B.

$$\begin{array}{ll} \wedge : \{0,1\} \times \{0,1\} & \to \{0,1\} \\ \vee : \{0,1\} \times \{0,1\} & \to \{0,1\} \\ \to : \{0,1\} \times \{0,1\} & \to \{0,1\} \\ \neg : \qquad \{0,1\} & \to \{0,1\} \end{array}$$

Ihre Werte lassen sich sehr einfach in Tabellenform darstellen:

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\to$	0	1
0	1	1
1	0	1

$\neg$	
0	1
1	0

Das bedeutet, wir können unsere Modelle als Funktionen auffassen:

$$M \subseteq Var \qquad \cong \qquad f_M : Var \to \{0,1\},$$

wobei gilt:

$$f_M(p) = 1 \text{ gdw. } p \in M$$

Man nennt f_M auch die **charakteristische Funktion** von M. Anstatt Mengen können wir also Funktionen als Modelle nehmen. Dann sieht das ganze so aus:

$f(\alpha \wedge \beta) = 1$, genau dann wenn $f(\alpha) = f(\beta) = 1$
$f(\alpha \vee \beta) = 1$, genau dann wenn $max\{f(\alpha), f(\beta)\} = 1$
$f(\neg\alpha) = 1$, gdw. $f(\alpha) = 0$
$f(\alpha \to \beta) = 1$, gdw. $max\{1 - f(\alpha), f(\beta)\} = 1$.

Oder noch kompakter:

$$\begin{aligned} f(\alpha \wedge \beta) &= min(f(\alpha), f(\beta) \\ f(\alpha \vee \beta) &= max(f(\alpha), f(\beta) \\ f(\neg\alpha) &= 1 - f(\alpha) \\ f(\alpha \rightarrow \beta) &= max(1 - f(\alpha), f(\beta)) \end{aligned}$$

Wir können dann schreiben: $f \models \alpha$ ist eine Abkürzung für $f(\alpha) = 1$.

Das schwache Prinzip der Wahrheitsfunktionalität folgt unmittelbar aus der Definition von Wahrheit. Wir können nun aber wiederum eine Induktion über die Formelkomplexität machen, und damit folgendes zeigen:

Prinzip der Wahrheitsfunktionalität, stark Die Wahrheit einer beliebigen Formel ist eine Funktion der Wahrheitswerte ihrer atomaren Teilformeln.

Das bedeutet: für jede Formel α gibt es eine Wahrheitstafel genau wie für die atomaren Konnektoren, nur dass wir eben den Wahrheitswert jeder Teilformel festlegen müssen. Wir können also z.B. folgende Tabelle erstellen für die Formel

$$\alpha = (p_1 \vee \neg p_2) \rightarrow p_3:$$

p_1	p_2	p_3	α
0	0	0	0
1	0	0	0
0	1	0	1
0	0	1	1
1	1	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Hier haben wir also die Wahrheitstabelle für eine komplexe Formel, und das Prinzip der Wahrheitsfunktionalität sagt uns, dass wir für *jede* Formel, egal wie lang, eine solche Wahrheitstabelle erstellen können.

Das bedeutet aber auch: jede Formel α mit n atomaren Propositionen kann man auffassen als eine Funktion

$$\alpha : \{0,1\}^n \to \{0,1\}$$

Das bedeutet: die Formel kann man als eine Funktion sehen. Wichtig ist: alle diese Semantiken sind äquivalent, insbesondere in Bezug auf das was gleich folgt.

5 Tautologien, Widersprüche etc.

Nachdem wir nun eine Semantik haben, können wir definieren was eine Tautologie und was ein Widerspruch ist:

1. Wir sagen, α ist eine **Tautologie**, falls gilt: für jedes $M \subseteq Var$, $M \models \alpha$
2. Wir sagen, α ist ein **Widerspruch**, falls gilt: für jedes $M \subseteq Var$, $M \not\models \alpha$
3. Wir sagen α ist **kontingent**, falls es Modelle $M, N \subseteq Var$ gibt, so dass $M \models \alpha$, $N \not\models \alpha$

Also gilt: Tautologien sind immer wahr, Widersprüche immer falsch, und nur kontingente Formeln sind manchmal wahr, und manchmal falsch. Es sind genau diese Formeln die uns Information über die Welt geben, da die Wahrheit einer Formel vom Zustand des Modells abhängt.

Ebenso sagen wir:

4. $\alpha \models \beta$, in Worten α **impliziert** β, falls gilt: falls $M \models \alpha$, dann gilt auch $M \models \beta$.

Das heißt also: jedes Modell von α ist ein Modell von β, anders gesagt, aus der Wahrheit von α folgt die Wahrheit von β.

Übung 2

Teil 1 Geben Sie eine Liste von 5 Tautologien, die jeweils mindestens drei verschiedene propositionale Variablen enthalten.

Teil 2 Geben Sie eine Liste von 5 Widersprüchen, die jeweils mindestens drei verschiedene propositionale Variablen enthalten.

Teil 3 Ist folgende Behauptung wahr oder falsch: falls α eine kontingente Formel ist, dann ist auch $\neg\alpha$ eine kontingente Formel. Begründen Sie!

Teil 4 Ist folgende Behauptung wahr oder falsch: falls α, β kontingente Formeln sind, dann ist auch $\alpha \to \beta$ eine kontingente Formel. Begründen Sie!

Teil 5 Gelten folgende Tautologien/Konsequenzen? Begründen Sie mit einer Semantik Ihrer Wahl!

1. $\neg(p \wedge q) \models \neg p \vee \neg q$
2. $(p \wedge q) \vee r \models (p \vee r) \wedge (q \vee r)$
3. $p \vee q \models \neg p \to q$
4. $((p \to q) \to q) \models q$
5. $(p \wedge q) \to r \models (p \to r) \vee (q \to r)$
6. $\models p \to (p \vee q)$

Hausaufgabe 1

Bitte bearbeiten bis zum 25.10.2021. Bearbeiten Sie Teil 1, 3, und Teil 5.4-5.6 der Übung!

6 Entscheidbarkeit

Das starke Prinzip der Wahrheitsfunktionalität ist sehr wichtig für Fragen der Entscheidbarkeit:

1. Ist α eine Tautologie?
2. Ist α ein Widerspruch?
3. Gilt $\alpha \models \beta$?

Im Prinzip besagt dieses Prinzip: im Grunde gibt es für eine Formel über n verschiedene propositionale Variablen nur 2^n nicht-äquivalente Modelle. Und wenn wir wissen wollen, ob eine Formel eine Tautologie ist, müssen wir nur diese 2^n Modelle prüfen, also alle Belegungen der verwendeten Variablen! Da wir das immer effektiv machen können, ist also Frage 1 entscheidbar.

Frage 2 ist ebenfalls entscheidbar: denn falls α ein Widerspruch ist, ist qua Definition $\neg\alpha$ ein Theorem – wir können also das Problem **reduzieren**.

Frage 3 ist ebenfalls entscheidbar: denn nimm an $\alpha \models \beta$, d.h. falls $M \models \alpha$, dann $M \models \beta$. Nimm also an $M \not\models \alpha$. Dann spielt es keine Rolle ob $M \models \beta$. Nimm an $M \models \alpha$. Dann muss auch gelten $M \models \beta$. Das bedeutet soviel wie: $\alpha \models \beta$ genau dann wenn $\alpha \to \beta \equiv \neg\alpha \vee \beta$ eine Tautologie ist!

7 Interdefinierbarkeit und funkionale Vollständigkeit

7.1 Interdefinierbarkeit

Wir haben gesehen wie man induktiv Wahrheitstafeln für Formeln erstellt. Mit deren Hilfe können wir auch neue logische Konnektoren **definieren**. Das ist hier ein technischer Begriff. Man nehme z.B. den Konnektor XOR, mit folgender Wahrheitstafel:

XOR	0	1
0	0	1
1	1	0

Das ist das sog. **exklusive oder**, das wahr ist genau dann wenn genau eines seiner Argumente wahr ist. Die Frage ist: wäre unsere Logik mächtiger, falls wir noch den Konnektor XOR hätten? Die Antwort lautet: **nein**, denn wir können ihn mittels unserer vorhandenen Konnektoren definieren. Das bedeutet: es gibt eine Formel $\alpha \in \texttt{WFF}$ über p, q so dass α dieselbe Wahrheitstafel hat wir $p\text{XOR}q$; in Symbolen schreiben wir:

$$\alpha \equiv p\text{XOR}q$$

Wie sieht diese Formel aus? Die Lösung lautet:

(1) $\alpha = (p \wedge \neg q) \vee (\neg p \wedge q)$

Es lässt sich leicht prüfen, dass α dieselbe Wahrheitstafel hat wie XOR. Das ist aber nur die Spitze des Eisbergs: wir können leicht sehen, dass sogar unsere bekannten Konnektoren interdefinierbar sind:

(2) $$p \vee q \equiv \neg(\neg p \wedge \neg q)$$

(3) $$p \wedge q \equiv \neg(\neg p \vee \neg q)$$

(4) $$p \rightarrow q \equiv \neg p \vee q$$

Wenn wir noch ein Symbol $\perp$ hinzunehmen, dessen Wahrheitswert immer $\perp$ ist, dann können wir sogar alle Konnektoren aus $\rightarrow$ definieren:

(5) $$\neg p \equiv p \rightarrow \perp$$

(6) $$p \vee q \equiv \neg p \rightarrow (\neg q \rightarrow \perp)$$

Das bedeutet – kurz gesagt: aus einer semantischen Perspektiv brauchen wir nur eine minimale Menge von Konnektoren, aus der wir alle anderen definieren können. Diese Mengen sind alternativ:

1. $\{\wedge, \neg\}$
2. $\{\vee, \neg\}$
3. $\{\rightarrow, \bot\}$

Jede dieser Mengen ist also semantisch gleichwertig, und wir können wahlweise eine von ihnen als gegeben, die anderen als definiert betrachten.

$(p \vee q) \vee r \equiv p \vee (q \vee r)$
$\neg\neg p \equiv p$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ (DeMorgan 1)
$\neg(p \vee q) \equiv \neg p \wedge \neg q$ (DeMorgan 2)

7.2 Funktionale Vollständigkeit

Wenn wir diese Begriffe haben, können wir uns fragen: gibt es einen beliebigen n-ären logischen Konnektor, den wir mittels unserer einfachen logischen Konnektoren nicht definieren können? Oder anders gefragt: gibt es eine Funktion ($\{0,1\}^n = \{0,1\} \times ... \times \{0,1\}$)

$$f : \{0,1\}^n \to \{0,1\}$$

die nicht einer logischen Formel entspricht? Die Antwort hierauf lautet: nein, jede **Boolesche Funktion** ist logisch definierbar. Wie zeigt man das? Die Antwort lautet: mittels Induktion, über n, die Anzahl der Argumente $\cong$ Anzahl benutzten propositionalen Variablen.

Induktionsbasis ist klar: es gibt nur 4 Funktionen $f : \{0,1\} \to \{0,1\}$, die wir alle aufschreiben können.

Induktionhypothese Nimm an, die Behauptung gilt für ein n.

Induktionsschritt Zunächst ist es wichtig zu wissen, dass eine Funktion

$$f : M \times N \to O$$

äquivalent ist zu einer Funktion

$$f : M \to (g : N \to O)$$

Man nennt dieses Verfahren **Currying** nach einem berühmten Logiker (Haskell Curry). Nimm nun an, wir haben eine Funktion

$$f : \{0,1\}^{n+1} \to \{0,1\},$$

also anders gesagt eine Funktion

$$f : \{0,1\} \to (g : \{0,1\}^n \to \{0,1\})$$

Das heißt: es gibt 2 Funktionen

$$g_0 = f(0) \tag{7}$$

$$g_1 = f(1) \tag{8}$$

Nach Induktionshypothese entsprechen g_0, g_1 jeweils einer Booleschen Formel α_0, α_1.

$$\begin{aligned} g_0 &\cong \alpha_0 \\ g_1 &\cong \alpha_1 \end{aligned}$$

Wir bauen uns jetzt eine Boolesche Formel für f:

$$(\neg p_{n+1} \to \alpha_0) \wedge (p_{n+1} \to \alpha_1)$$

Das bildet über die Curry-Äquivalenz genau unsere Formel f ab. $\dashv$

Das bedeutet:

Satz 2 *Jede Boolesche Funktion lässt sich mit einer aussagenlogischen Formel beschreiben.*

Dieser Satz ist sehr wichtig für unsere Computer, die ja im Prinzip nur Boolesche Funktionen berechnen, und dabei nur auf logische Konnektoren zurückgreifen können!

Übung 3

Teil 1 Definieren Sie folgende Konnektoren:

1. X1, ein ternärer Konnektor mit folgender Tabelle:

p_1	p_2	p_3	$X1(p_1, p_2, p_3)$
0	0	0	1
1	0	0	0
0	1	0	1
0	0	1	0
1	0	1	0
1	1	0	1
0	1	1	1
1	1	1	0

2. X2, ein ternärer Konnektor mit folgender Tabelle:

p_1	p_2	p_3	$X2(p_1, p_2, p_3)$
0	0	0	1
1	0	0	0
0	1	0	1
0	0	1	0
1	0	1	1
1	1	0	1
0	1	1	1
1	1	1	0

3. X3, ein ternärer Konnektor mit folgender Tabelle:

p_1	p_2	p_3	$X2(p_1, p_2, p_3)$
0	0	0	0
1	0	0	0
0	1	0	0
0	0	1	1
1	0	1	1
1	1	0	0
0	1	1	1
1	1	1	0

Lösung 3: Wir nähern uns der korrekten Tabelle am besten von unten, indem wir für jede Zeile mit einer 1 eine Teilformel schreiben:

$$
\begin{aligned}
&(\neg p_1 \wedge \neg p_1 \wedge p_3)\\
\vee&(p_1 \wedge \neg p_1 \wedge p_3)\\
\vee&(\neg p_1 \wedge p_1 \wedge p_3)
\end{aligned}
$$

Teil 2 Jede Wahrheitstabelle entspricht einer aussagenlogischen Formel, und umgekehrt hat jede aussagenlogische Formel eine Wahrheitstabelle. Sei $\texttt{WFF}_4$ die Menge aller aussagenlogischen Formeln mit nur den Variablen p_1, p_2, p_3, p_4.

- Wie viele solcher Formeln gibt es, die nicht logisch äquivalent sind (also wie größ ist die größte Menge solcher Formeln, in der keine zwei Formeln logisch äquivalent ist)?
- Und wie ist das für im Allgemeinen Fall für $\texttt{WFF}_n$?

Teil 3

- Finden Sie eine Formel $\alpha \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ (also semantisch äquivalent), wobei α nur die Konnektoren $\rightarrow, \perp$ nutzen darf!

8 Tableau Methoden und Entscheidbarkeit

Wir haben bereits gesehen, dass wir alle wichtigen Probleme der Aussagenlogik mittels unserer Wahrheitstafeln entscheiden können. Das Problem dabei ist: das ist sehr mühsam. Denn wenn wir n propositionale Variablen in einer Formel haben, dann bekommen wir 2^n Zeilen in der Tabelle, was sehr schnell sehr viele werden.

Oftmals haben wir das Gefühl, ein Beweis funktioniert intuitiv einfacher; insbesondere haben wir ja den Abschluss unter Substitution: $\alpha \vee \neg\alpha$ ist eine Tautologie für beliebige α! Unsere Wahrheitstafeln nutzen diese Tatsache aber nicht.

Das Problem ist dass wir trotzdem einen formalen Beweis möchten. Hier helfen und Tableaus, die tatsächlich in vielen Fällen eine einfachere Lösung bieten.

Beth-Tableaus sind eine Methode, um zu entscheiden ob

$$\alpha \models \beta$$

gilt. Damit kann man auch als Spezialfall prüfen ob α eine Tautologie oder Widerspruch ist, denn in dem Fall haben wir

$$\models \alpha \text{ bzw. } \alpha \models,$$

wobei eine Seite leer bleibt. Die Idee hinter diesen Tableaus ist, dass wir eine **Belegung** suchen, die

1. α wahr und
2. β falsch macht

Wenn es *keine* solche Belegung gibt, gilt $\alpha \models \beta$. Das funktioniert wie folgt: um zu zeigen, ob $\alpha \models \beta$ gilt, nehmen wir erst mal das Gegenteil an, nämlich:

$$\alpha \text{ ist wahr, } \beta \text{ ist falsch!}$$

Z.B. für $p \to \neg q \models \neg(p \wedge q)$

wahr	falsch
$p \to \neg q$	$\neg(p \wedge q)$
$p \wedge q$	
p	
q	
$\neg q$ |	| p
Widerspruch!	Widerspruch!

Wir haben also das Tableau mit einem Widerspruch geschlossen, denn das tableau sagt: q und $\neg q$ sind wahr; und p ist wahr und p ist falsch. Wichtig sind hier die Regeln:

- Die Negation lässt sich eliminieren, indem wir die Formel von wahr nach falsch schieben, und umgekehrt.
- Die Konjunktion $p \wedge q$ lässt sich auf der wahr-Seite einfach auflösen nach p, q, denn beide müssen wahr sein.

Die anderen Konnektoren sind etwas komplizierter. Wichtig ist: am Ende müssen wir das Tableau schließen, also einen Widerspruch finden. Das bedeutet: die Belegung, die α wahr und β falsch macht, existiert nicht, denn sie müsste sowohl z.B. p wahr als auch p falsch machen. Tableaus beruhen also auf dem Beweis durch Widerspruch: nimm an, eine Belegung macht α wahr, β falsch. Das führt auf einen Widerspruch. Also gibt es diese Belegung nicht. Also macht jede Belegung, die α wahr macht, auch β wahr.

Die Methode der Tableaus beruht weiterhin darauf, komplexe Formeln auf atomare Propositionen aufzulösen. Das ist aber nicht immer notwendig: im obigen Tableau könnten auch komplexe Formeln für p, q stehen, und wir hätten das Tableau bereits geschlossen. Das heißt es kann wesentlich schneller gehen, und das ein Großer Vorteil von Tableaus über Wahrheitstafeln; der zweite ist, dass wir gezielt Strategien anwenden können.

1. Wir müssen in Tableaus nicht immer bis zu atomaren Propositionen runtergehen, es reicht für beliebige Formeln α den Widerspruch α wahr, α falsch zu finden.
2. Wir können unserer Intuition folgen, um eine optimale Lösung zu finden.

Diese beiden Gründe führen dazu, dass Tableau oft viel praktischer sind (und kleiner) als Beweise über Wahrheitstafeln, die für n propositionale Variablen zu 2^n Einträgen führen, und die man nicht sinnvoll komprimieren kann. Wir haben aber bislang nur die einfachen Regeln besprochen, es wird noch etwas komplizierter.

Betrachten wir obiges Tableau. Dann sehen wir, dass wir in der vorletzten Zeile die Spalten wiederum getrennt haben. Diese Trennung bedeutet eine **Fallunterscheidung**: zu sagen dass die Implikation $p \to q$ wahr ist, bedeutet soviel wie: entweder p ist falsch, oder q ist wahr. Das bedeutet: wir

teilen das eine Tableau in zwei **Subtableau** (links und rechts), und müssen *beide* auf einen Widerspruch führen um das Tableau zu schließen. Diese Split-Methode braucht man auch bei anderen Konnektoren:

- Eine Implikation $p \to q$ auf der wahr-Seite führt zu einem Split: links q auf wahr, rechts p auf falsch.
- Eine Disjunktion $p \vee q$ auf der wahr-Seite führt zu einem Split: links p auf wahr, rechts q auf wahr.
- Eine Konjunktion $q \wedge q$ auf der falsch-Seite führt zu einem Split: links p auf falsch, rechts q auf falsch.

Das sind die Split-Regeln. Jetzt fehlen tatsächlich nur noch 2:

- Aus einer Disjunktion $p \vee q$ auf der falsch-Seite können wir p und q auf der falsch-Seite folgern.
- Aus einer Implikation $p \to q$ auf der falsch-Seite können wir p auf der wahr-Seite, q auf der falsch-Seite folgern.

Nun haben wir alles beisammen; hier nochmal der Überblick:

Konnektor	wahr	falsch
$\neg\alpha$	α nach falsch	α nach wahr
$\alpha \wedge \beta$	α, β nach wahr	Split: α falsch, β falsch
$\alpha \vee \beta$	Split: α wahr, β wahr	α, β nach falsch
$\alpha \to \beta$	Split: α nach falsch, β nach wahr	α nach wahr, β nach falsch

Ziel ist es, jedes Subtableau zu schließen, d.h. im selben Subtableau entweder

- $p, \neg p$ unter wahr/falsch zu bekommen, oder
- p oder wahr und p unter falsch zu bekommen

Wenn wir das Tableau für α, β schließen (d.h. alle Subtableaus), dann gilt $\alpha \models \beta$. Wenn wir α, β bis auf atomare Propositionen runtergebrochen haben und das Tableau nicht geschlossen ist, dann gibt es eine Belegung, die α wahr, β falsch macht, also gilt:

$$\alpha \not\models \beta$$

Außerdem gilt: ihr Tableau sagt Ihnen genau, welche Propositionen man mit 1, welche mit 0 belegen muss, um die Implikation zu falsifizieren.

Wichtig ist: für jedes Tableau gibt es immer eine Korrespondenz wahr/falsch: für ein einfaches Tableau reicht es, eine Spalte zu schließen. Für ein gespaltenes reichen 2 Spalten, aber eben 2 Spalten, die nicht miteinander in Korrespondenz stehen (siehe Beispiel oben!).

Noch eine wichtige Eigenschaft gibt es: nehmen wir an, Sie haben ein Tableau mit einer Formel

$$\alpha, \neg\alpha$$

im selben Subtableau. Dann können Sie natürlich das Tableau weiterführen, bis Sie nur noch atomare Propositionen haben. In diesem Fall können Sie aber das Tableau auch schon **direkt schließen**, denn kein Belegung kann sowohl α wahr als auch $\neg\alpha$ wahr/falsch machen!

Ebenso falls α sowohl unter wahr als auch unter falsch zu finden ist. Das weitere Hinunterbrechen bis zu Atomen ist also nur dann wirklich nötig, falls Sie Ihr (Sub)Tableau nicht bereits vorher schließen können.

Wichtige Merkregeln zu Beth-Tableaus Hier einige Merksätze zu Tableaus:

- Jeder Fall besteht aus 2 Seiten, wahr und falsch (so wie ein Blatt Papier). Jede Fallunterscheidungsregel teilt das Tableau sowohl auf der wahr- als auch der falsch-Seite! (wie wenn man das Blatt zerreisst)

- Um einen Fall zu schliessen, muss man *nur eine* der beiden Seiten auf einen Widerspruch führen. Das bedeutet dann: in diesem Fall (also beide Seiten!) haben wir einen Widerspruch.

- Die Wahrheit läuft *nach unten*: jede Formel, die oberhalb einer Fallunterscheidung steht, gilt in allen unterstehenden Fällen (d.h. ist wahr im Fall auf der wahr-Seite, falsch im Fall auf der falsch-Seite).

- Nimm an, ich habe eine unverbrauchte Formel, die eine Fallunterscheidung zeitigt, oberhalb einer Fallunterscheidung. Z.B. $\alpha \vee \beta$ auf der wahr-Seite, und darunter unterscheide ich Fall 1/Fall 2. Wenn ich jetzt die Formel $\alpha \vee \beta$ auflöse, dann habe ich eine eingebettete Fallunterscheidung:

Fall 1.1 α | Fall 1.2 β | Fall 2.1 α | Fall 2.2 β

Das gilt aber nur für Fallunterscheidungen, die *unterhalb* der entsprechenden Formel stehen!

- Denn: die Wahrheit (und Falschheit) schwappt nicht über: was nur unter Fall 2 steht, kommt niemals nie nach Fall 1, weder wahr noch falsch.

Hier noch ein paar Tipps zur "**Buchhaltung**":

- Alle Zeilen im Tableau sind nummeriert (sagen wir links)
- Dazu kommt noch eine Spalte, wo wir für jede neue Zeile sagen (also alle Zeilen ausser 1), woher die gewonnene Formel kommt (Zeile Spalte, also nw bzw. nf). Auf jede Formel im Tableau kann man immer genau eine Regel anwenden, wenn ich also weiß, woher eine Formel kommt, ist das Tableau perfekt nachvollziehbar!
- Das Ziel des Tableau ist es ja, aus komplexen Formeln atomare Formeln zu machen bzw. negierte atomare Formeln. Da man auf jede Formel immer nur eine Regel anwenden kann, macht es keinen Sinn diese Regel mehr als einmal auf dieselbe Formel anzuwenden. Daher ist es sinnvoll, zu markieren ob man eine Formel bereits "**verbraucht**" hat oder nicht.
- Am besten einfach die Formel bzw. deren obersten Konnektor durchstreichen (aber lesbar lassen!), so weiß man dass diese Formel nicht mehr benutzt werden muss!

Übung 4

Beweisen Sie mittels Beth Tableaux, ob folgende Implikationen gelten:

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

5. $(p_1 \vee p_2) \to \neg(p_3 \wedge p_4) \models p_1 \to \neg p_3$

6. $p_1 \wedge \neg(p_2 \vee p_3) \models \neg p_2$

7. $\neg(p \to (q \wedge r)) \models p \wedge (\neg q \vee \neg r)$

8. $\neg((p_1 \wedge \neg p_2) \vee p_3) \models (p_1 \wedge p_2) \to p_3$

9. Hart: $(\neg(p \wedge q)) \vee (p \wedge \neg q) \models (\neg(p \to q)) \wedge (\neg(q \to p))$

9 Noch eine Semantik: Boolesche Algebren

9.1 Strukturtheorie

Auch wenn wir erstmal keinen Bedarf an einer weiteren (äquivalenten) Semantik verspüren, gibt es eine, die man unmöglich auslassen kann, nämlich die sog. Booleschen Algebren. Hier ist wiederum eine kleine Änderung in der Perspektive nötig. Anstatt von der Wahrheit einer Formel in einem Modell zu sprechen, sprechen wir von der **Bedeutung einer Formel**, die wie folgt definiert ist: aus

$$M \models \alpha$$

wird

$$\|\alpha\| = \{M : M \models \alpha\}$$

Wir sagen also: die Bedeutung einer Formel ist die Menge aller Modelle, in denen sie wahr ist. Diese Bedeutungsdefinition erlaubt ebenfalls eine induktive Definition der Konnektoren:

$$\begin{array}{lcl}
\|p\| & = & \{M \subset \mathit{Var} : p \in M\} \\
\|\alpha \wedge \beta\| & = & \|\alpha\| \cap \|\beta\| \\
\|\alpha \vee \beta\| & = & \|\alpha\| \cup \|\beta\| \\
\|\neg\alpha\| & = & \wp(\mathit{Var}) - \|\alpha\|, \text{ wobei } \wp \text{ die Potenzmenge ist} \\
\|\alpha \to \beta\| & = & (\wp(\mathit{Var}) - \|\alpha\|) \cup \|\beta\|
\end{array}$$

Dann gilt:

Lemma 3 *$M \models \alpha$ gdw. $M \in \|\alpha\|$.*

Das bringt uns zum Begriff der **Booleschen Algebra**: Boolesche Algebren sind Modelle für Bedeutungen von klassischer Logik. Hier werden logische Operationen direkt als Operationen definiert, wobei die normalen Operation sind: $\cup$, $\cap$, $\overline{[-]}$; außerdem gibt es Konstanten $0, 1$. Eine Boolesche Algebra ist also eine Algebra

$$\mathbf{B} = (B, \cup, \cap, \overline{[-]}, 0, 1)$$

wobei $\cup, \cap$ binäre Funktionen sind, $\overline{[-]}$ unär. Wohlgemerkt: es handelt sich hier im Allgemeinen *nicht* um die mengentheoretischen Operationen, wir benutzen nur dieselben Symbole! Die Eigenschaften der Operatoren werden durch folgende Axiome geregelt:

($\cap$1)	$a \cap b = b \cap a$	($\cup$1)	$a \cup b = b \cup a$
($\cap$2)	$a \cap (b \cap c) = (a \cap b) \cap c$	($\cup$2)	$a \cup (b \cup c) = (a \cup b) \cup c$
($\cap$3)	$a \cap a = a$	($\cup$3)	$a \cup a = a$
($\cap$4)	$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$	($\cup$4)	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
($\cap$5)	$a \cap 1 = a$	($\cup$5)	$a \cup 0 = a$
($\cap$6)	$a \cap 0 = 0$	($\cup$6)	$a \cup 1 = 1$
($\cap$7)	$a \cap \overline{a} = 0$	($\cup$7)	$a \cup \overline{a} = 1$
(DN)	$\overline{\overline{a}} = a$		
(DM1)	$\overline{(a \cap b)} = \overline{a} \cup \overline{b}$	(DM2)	$\overline{(a \cup b)} = \overline{a} \cap \overline{b}$
(Du1)	$\overline{0} = 1$	(Du2)	$\overline{1} = 0$
(Abs1)	$a \cap (a \cup b) = a$	(Abs2)	$a \cup (a \cap b) = a$

Dieses Axiomensystem ist hochgradig redundant (es geht auch mit nur 3 Axiomen), gibt aber ein gutes Verständnis von Booleschen Algebren. Was man dabei insbesondere sieht ist folgendes:

Prinzip der Dualität Nimm eine beliebige Gleichung $s = t$, die in allen Booleschen Algebren wahr ist. Bilde s' (und t') indem

1. alle Vorkommen von $\cap$ durch $\cup$ ersetzt werden,
2. alle Vorkommen von $\cup$ durch $\cap$ ersetzt werden,
3. alle Vorkommen von 1 durch 0 ersetzt werden,
4. alle Vorkommen von 0 durch 1 ersetzt werden.

Dann ist $s' = t'$ ebenso wahr in allen Booleschen Algebren.

Wir nennen t' den dualen Term zu t. Natürlich gilt: $t'' = t$, also gilt: eine Gleichung ist wahr genau dann wenn die duale Gleichung wahr ist.

Beispiel 1 Das erste und auch wichtigste Beispiel für eine Boolesche Algebra ist folgende: wir setzen

$$B = \{0, 1\}$$

Damit sind bereits alle Operationen definiert. Nennen wir diese Algebra $\mathbf{B}_1$. Wir werden später sehen, dass die wahrheitsfunktionale Semantik nichts weiter ist als die Interpretation von Formeln in die Algebra $\mathbf{B}_1$.

Beispiel 2 Nimm eine beliebige Menge, z.B. die Menge $M = \{a, b\}$. Wir lassen nun die Trägermenge $\wp(M)$ sein, also die Potenzmenge. Nun definieren wir die Boolesche Algebra $(\wp(M), \cap, \cup, \overline{[-]}, \emptyset, M)$, wobei die Operationen einfach die bekannten mengentheoretischen sind. Einfachheit halber nennen wir diese Algebra $\wp(M)$, genau wie die Potenzmenge selbst.

Beispiel 3 Es gibt aber noch viele andere abstraktere Algebren. Eine solche Algebra werden wir jetzt präsentieren: erinnern wir uns dass $\alpha \equiv \beta$ bedeutet, dass $\alpha \models \beta$, $\beta \models \alpha$. Wir können nun **Äquivalenzklassen** definieren:

$$\alpha_{\equiv} = \{\beta : \alpha \equiv \beta\}.$$

Zuletzt definieren wir die Menge aller Äquivalenzklassen von Formeln:

$$\mathtt{WFF}_{\equiv} = \{\alpha_{\equiv} : \alpha \in \mathtt{WFF}\}$$

Diese Menge bildet eine Boolesche Algebra: wir definieren

- $M \cup N = (\alpha \vee \beta)_{\equiv}$ für ein beliebiges $\alpha \in M, \beta \in N$,
- $M \cap N = (\alpha \wedge \beta)_{\equiv}$ für ein beliebiges $\alpha \in M, \beta \in N$,
- $\overline{M} = (\neg\alpha)_{\equiv}$ für ein beliebiges $\alpha \in M, \beta \in N$
- $1 = (p \vee \neg p)_{\equiv}$ für ein beliebiges p
- $0 = (p \wedge \neg p)_{\equiv}$ für ein beliebiges p

Die Formelalgebra $(\mathtt{WFF}_{\equiv}, \cap, \cup, \overline{[-]}, 0, 1)$ ist tatsächlich eine Boolesche Algebra. Es ist eine sehr sinnvolle und interessante Übung zu zeigen, dass diese Algebra mit den Operationen, so wie oben definiert, tatsächlich eine Boolesche Algebra ist.

Eine Konvention Eine wichtige Konvention ist folgende: wir schreiben

$$a \leq b$$

mit der Bedeutung:

$$a \cup b = b, \text{ äquivalent } a \cap b = a.$$

- Die Relation $\leq$, in Booleschen Algebren, ist soz. das algebraische Gegenstück zum logischen $\models$.
- Das logische $\perp$ entspricht der algebraischen 0, als das kleinste bzw. "falscheste" Objekt.

Mittels dieser Definition kann man $\cap, \cup, \overline{[-]}$ ordnungstheoretisch definieren; sogar

$$a \Rightarrow b := \overline{a} \cup b$$

lässt sich derart definieren:

1. $a \cup b$ ist das kleinste Objekt, dass größer als a und b ist.
2. $a \cap b$ ist das größte Objekt, dass kleiner als a und b ist.
3. $\overline{a}$ ist das kleinste Objekt, so dass $a \cup \overline{a} = 1$
4. $a \Rightarrow b$ ist das größte Objekt so dass $(a \Rightarrow b) \cap a \leq b$.

Einige wichtige (Un)gleichungen Folgende Gleichungen gelten in allen Booleschen Algebren:

$$\overline{\overline{a} \cup \overline{b}} = a \cap b \tag{9}$$

$$\overline{\overline{a} \cap \overline{b}} = a \cup b \tag{10}$$

$$a = (a \cap b) \cup (a \cap \overline{b}) \tag{11}$$

$$a = (a \cup b) \cap (a \cup \overline{b}) \tag{12}$$

$$a \cup b = a \cup (\overline{a} \cap b) \tag{13}$$

$$a \cap b = a \cap (\overline{a} \cup b) \tag{14}$$

$$\overline{(a \cap b) \cup (\overline{a} \cap \overline{b})} = (a \cap \overline{b}) \cup (b \cap \overline{a}) \tag{15}$$

$$\overline{(a \cup b) \cap (\overline{a} \cup \overline{b})} = (a \cup \overline{b}) \cap (b \cup \overline{a}) \tag{16}$$

$$\overline{b \cap c} \leq \overline{a \cap b} \cup \overline{c} \tag{17}$$

Weiterhin gilt:

(18) $a \leq b \qquad \Longleftrightarrow \qquad \overline{b} \leq \overline{a}$

Außerdem gibt es folgende, in gewissem Sinn zentrale Sätze für Boolesche Algebren:

Satz 4 *Eine Gleichung $s = t$ gilt in allen Booleschen Algebren, genau dann wenn sie in $\boldsymbol{B}_1$ gilt.*

Das bedeutet, im Prinzip gelten alle wesentlichen Gesetze bereits in $\mathbf{B}_1$, und aus logischer Perspektive gibt es keinen Grund, sich komplexere Algebren anzuschauen. Der nächste Satz ist ein sog. Repäsentationstheorem, da es besagt wie wir (abstrakte) Algebren (konkret) repräsentieren können:

Satz 5 *Jede endliche Boolesche Algebra (d.h. mit endlicher Trägermenge) ist isomorph (d.h. gleich bis auf Benennung der Objekte) mit einer Algebra der Form $\wp(M)$, für M eine endliche Menge.*

Beweis (Skizze) Man nennt die Objekte $a \in B$, so dass gilt: $0 < a$, aber für alle $b \neq 0$ gilt $b \not< a$ auch **Atome**. Atome sitzen also unmittelbar über der 0. Wir nennen die Atome einer Algebra $\mathbf{B}$ auch $A(\mathbf{B})$

Schritt 1:

Es gilt in allen *endlichen* Booleschen Algebren $\mathbf{B}$, für alle $b \in B$:

(19) $b = \bigvee \{a \in A(\mathbf{B}) : a \leq b\}$

$\geq$ ist klar, $\leq$ ist ein einfaches Argument mit Komplement $\overline{b}$. Das bedeutet: Jedes Objekt einer endlichen BA ist genau bestimmt durch die Atome, die es "dominiert".

Schritt 2:

Sei also $\mathbf{B}$ eine endliche BA, $A(\mathbf{B})$ die Menge ihrer Atome. Dann ist natürlich

(20) $\wp(A(\mathbf{B}))$

eine Boolesche Algebra (Potenzmengenalgebra), und weiterhin gilt: die Abbildung

(21) $i(b) = \{a \in A(\mathbf{B}) : a \leq b\}$

ist ein **Isomorphismus**, d.h. eine Bijektion so dass

$$\begin{aligned} i(b_1 \cup b_2) &= i(b_1) \cup i(b_2) \\ i(b_1 \cap b_2) &= i(b_1) \cap i(b_2) \\ i(\overline{b_1}) &= \overline{i(b_1)} \\ i(1) &= A(\mathbf{B}) \\ i(0) &= \emptyset \end{aligned}$$

Das muss man natürlich noch beweisen! **Ende der Skizze**

Isomorphie bedeutet also soviel wie Strukturgleichheit, d.h. alles bleibt gleich, nur die Objekte werden eindeutig umbenannt. Der letzte Satz besagt unter anderem:

1. Jede endliche BA hat, für ein bestimmtes $n \in \mathbb{N}$, 2^n Elemente in der Trägermenge.

2. Alle Booleschen Algebren mit 2^n Elementen ($n \in \mathbb{N}$) sind isomorph, also strukturgleich.

Diese Ergebnisse könnten den Eindruck erwecken, dass Boolesche Algebren relativ banal sind; das stimmt aber ganz und gar nicht. Besonders im unendlichen Fall gibt es sehr spannende Strukturen: z.B. die Algebra über $\wp(\mathbb{N})$, wobei jedes Objekt die Form hat

$$\uparrow M = \{n \cdot m : m \in M, n \in \mathbb{N}\}$$

D.h. jede Menge basiert auf einer Menge von Zahlen und allen ihren Vielfachen. Die 0 ist die leere Menge $\emptyset$, die 1 ist $\mathbb{N}$, $\cup$ und $\cap$ werden mengentheoretisch aufgefasst. Diese Algebra hat z.B. keine **Atome**, d.h.: für alle Objekte $a \neq 0$ der Algebra gibt es ein b so dass $0 < b < a$. Z.B. ist

$$\uparrow\{2\} \cap \uparrow\{3\} = \uparrow\{6\},$$

allgemeiner:

$$\uparrow\{m\} \cap \uparrow\{n\} = \uparrow\{m \cdot n\},$$

Der Schnitt basiert also auf dem kgv, die Vereinigung $\cup$ auf dem ggt.

9.2 Interpretation von Formeln in Algebren

Nun sollte klar sein, wie man eine Formel aus `WFF` in eine BA interpretiert. Man macht das normalerweise mittels einer Funktion

$$\sigma : Var \to B,$$

die erweitert wird auf beliebige Formeln mittels

$$\begin{array}{lcl}
\underline{\sigma}(\alpha \wedge \beta) & = & \underline{\sigma}(\alpha) \cap \underline{\sigma}(\beta) \\
\underline{\sigma}(\alpha \vee \beta) & = & \underline{\sigma}(\alpha) \cup \underline{\sigma}(\beta) \\
\underline{\sigma}(\neg\alpha) & = & \overline{\underline{\sigma}(\alpha)} \\
\underline{\sigma}(\alpha \to \beta) & = & \overline{\underline{\sigma}(\alpha)} \cup \underline{\sigma}(\beta)
\end{array}$$

Das bedeutet soviel wie: die Interpretation $\| - \|$, die wir Eingangs erwähnt haben, ist eine Boolesche-Algebra Interpretation; die Algebra ist $\wp(\wp(Var))$. Diese Algebra ist in gewissen Sinne kanonisch, und man nennt Mengen der Form $\underline{\sigma}(\alpha)$ auch **mögliche Welten** (dazu ein andermal mehr).

Ein algebraisches Modell ist also ein Paar $(\mathbf{B}, \sigma)$, wobei $\mathbf{B}$ eine Boolesche Algebra ist, σ die Interpretation. Wir schreiben

$$\alpha \models_{(\mathbf{B},\sigma)} \beta \qquad \Longleftrightarrow \qquad \underline{\sigma}(\alpha) \leq_{\mathbf{B}} \underline{\sigma}(\beta)$$

Hier ist $\leq_{\mathbf{B}}$ die entsprechende Relation der Booleschen Algebra $\mathbf{B}$. Wir können nun auch sehen, dass die algebraische Semantik alle vorangehenden verallgemeinert: die Wahrheitssemantik basiert auf Interpretationen in $\mathbf{B}_1$, und die mengentheoretischen Modelle entsprechen der Semantik, die wir hier vorstellen. Dementsprechend schreiben wir:

$$\alpha \models \beta, \text{ gdw. für alle } (\mathbf{B}, \sigma),\ \alpha \models_{(\mathbf{B},\sigma)} \beta$$

Und das ist wiederum äquivalent zu der Relation $\models$ wie wir sie bereits definiert haben.

Hausaufgabe 4

Bitte bearbeiten bis zum 15.11.2021.

1. Beweisen Sie die (Un)gleichungen 16, 17. Formen Sie hierfür die Terme Schritt für Schritt um. Jeder Umformungsschritt soll hierbei durch ein Boolesches Axiom gedeckt sein; schreiben Sie das entsprechende Axiom neben die Umformung.

2. Beweisen Sie dass $\overline{b} \leq \overline{a}$ impliziert $a \leq b$.

Übung

Zeichnen Sie das Hasse Diagramm für die Boolesche Algebra $\wp(\{a, b, c\})$!

Übung zum 17.11.2021

1. Zeichnen Sie dass Hasse Diagramm für die Boolesche Algebra mit 4 Atomen (also 2^4 Elementen).

2. Beweisen Sie, dass in allen Booleschen Algebren gilt:

$$a \cap b = 0 \text{ gdw. } b \leq \overline{a}$$

(anders gesagt: $\overline{a}$ ist das größte Element c so dass $a \cap c = 0$)

Kleine Hilfe: für 1, denken Sie an die Aufgabe zu Mittwoch, für 2, denken Sie an die Repräsentation mittels Potenzmengen!

10 Beweistheorie

10.1 Allgemeines

Wir sind nun fertig mit der Semantik von Formeln; wir kommen nun zu der Theorie der formalen Beweise. Hierfür werden Formeln nicht interpretiert, sondern als rein syntaktische Objekte behandelt. Um diese Theorie von der Semantik zu trennen, benutzt man ein anders Symbol, nämlich $\vdash$, was soviel bedeutet wie: logische Konsequenz – aber eben rein syntaktisch. Uns interessieren 3 Fragen:

1. Ist α ein Theorem, also $\vdash \alpha$? Das bedeutet soviel wie: α ist **beweisbar**.
2. Ist α ein Widerspruch, also $\alpha \vdash$? Das bedeutet soviel wie: aus α lässt sich alles beweisen.
3. Gegeben eine Menge Γ von Formeln, lässt sich unter der Annahme von Γ eine Formel α beweisen? Dann schreiben wir $\Gamma \vdash \alpha$.

Das Ziel am Ende ist **Vollständigkeit**, das bedeutet: wir möchten zeigen dass $\alpha \vdash \beta$ gdw. $\alpha \models \beta$. Das heißt mit anderen Worten: Theoreme sollen Tautologien sein, Beweisbarkeit soll mit Wahrheit zusammenfallen.

Eine gute Frage : wofür brauchen wir ein Beweiskalkül, wenn unsere Semantik mittels z.B. Beth Tableau bereits eine effektive und einigermaßen effiziente Methode liefert, um zu entscheiden ob $\alpha \models \beta$?

Die Antwort : der semantische Beweis funktioniert nur für Aussagenlogik in dieser einfachen Form; sobald wir Quantoren einführen, wird das nicht mehr gehen. Der Beweiskalkül wird auch in diesem Fall funktionieren!

10.2 Der Kalkül CL

Wir präsentieren nun den sog. **Sequentenkalkül** CL, erstmal ohne viele Worte. Wir haben ein Axiom, das uns besagt, dass der Sequent $p \vdash p$ immer ableitbar ist. Die übrigen Regeln sind Regeln, die uns sagen, wie wir aus ableitbaren **Sequenten** neue Sequenten ableiten können. Diese Regeln erlauben uns, Baumartige Strukturen zu bilden, die wir **Beweise** (in einem formalen Sinne) nennen.

Wichtig ist an dieser Stelle: die Relation '$\vdash$' setzt zwei *Mengen* in Beziehung. In der üblichen Notation wird das aber nicht wirklich deutlich. Daher gilt:

$$p \vdash p$$

ist eine Abkürzung für

$$\{p\} \vdash \{p\}$$

Man benutzt oft große griechische Buchstaben als Abkürzungen für Mengen von Formeln; man schreibt dann

$$\Gamma, \alpha \vdash \Delta, \beta$$

als eine Abkürzung für

$$\Gamma \cup \{\alpha\} \vdash \Delta \cup \{\beta\}$$

usw. für alle möglichen Folgen von großen/kleinen griechischen Buchstaben. Objekte der Form $\Gamma \vdash \Delta$ nennt man **Sequenten**, daher der Name.

(ax) $\dfrac{}{p \vdash p}$

$$(\wedge\mathrm{I})\ \frac{\Gamma, \alpha, \beta \vdash \Theta}{\Gamma, \alpha \wedge \beta \vdash \Theta} \qquad (\mathrm{I}\wedge)\ \frac{\Gamma \vdash \Theta, \alpha \quad \Gamma \vdash \Theta, \beta}{\Gamma \vdash \Theta, \alpha \wedge \beta}$$

$$(\vee\mathrm{I})\ \frac{\Gamma, \alpha \vdash \Theta \quad \Gamma, \beta \vdash \Theta}{\Gamma, \alpha \vee \beta \vdash \Theta} \qquad (\mathrm{I}\vee)\ \frac{\Gamma \vdash \Theta, \alpha, \beta}{\Gamma \vdash \Theta, \alpha \vee \beta}$$

$$(\neg\mathrm{I})\ \frac{\Gamma \vdash \Delta, \alpha}{\neg\alpha, \Gamma \vdash \Delta} \qquad (\mathrm{I}\neg)\ \frac{\Gamma, \alpha \vdash \Delta}{\Gamma \vdash \Delta, \neg\alpha}$$

$$(\rightarrow\mathrm{I})\ \frac{\Gamma, \alpha \vdash \Delta \quad \Theta \vdash \beta}{\Gamma, \Theta, \beta \rightarrow \alpha \vdash \Delta} \qquad (\mathrm{I}\rightarrow)\ \frac{\Gamma, \alpha \vdash \beta, \Delta}{\Gamma \vdash \alpha \rightarrow \beta, \Delta}$$

Nachtrag für Fortgeschrittenere Das war übrigens die "pädagogische Version von ($\rightarrow$I); die "volle Version" geht so:

$$(\rightarrow\mathrm{I})\ \frac{\Gamma, \alpha \vdash \Delta \quad \Theta \vdash \beta, \Delta}{\Gamma, \Theta, \beta \rightarrow \alpha \vdash \Delta}$$

Die ist weniger intuitiv, braucht man aber manchmal! Natürlich lässt sich hiermit (mit (weak)) die pädagogische Regel leicht simulieren.

Jetzt fehlen nur noch zwei Arten von Regeln, die aber von enormer Wichtigkeit sind:

$$(\mathrm{weak})\ \frac{\Gamma \vdash \Delta}{\Gamma, \Theta \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \Theta}$$

(weak) ist eine Regel, die besagt: wir können immer (unnötige) Prämissen zu unserem Beweis hinzunehmen, er bleibt dadurch gültig (die rechte (weak)-Regel ist nur das Dual dazu). Und zuletzt der sog. Schnitt:

$$(\mathrm{schnitt})\ \frac{\Gamma \vdash \alpha, \Delta \quad \Theta, \alpha \vdash \Psi}{\Theta, \Gamma \vdash \Delta, \Psi}$$

(schnitt) ist eine Art *copy-paste*-Regel: sie besagt, dass wir Teilbeweise (wie

$\Gamma \vdash \alpha$, die wir separat anfertigen, in andere Beweise einkleben können, indem wir die **Schnittformel** α ersetzen durch Γ.

Das wars auch schon (im Prinzip). Denn durch die Tatsache, dass $\vdash$ eine Relation zwischen Mengen ist, gibt es zwei wichtige Regeln soz. "aufs Haus", d.h. wir können sie anwenden, ohne dass wir sie explizit in den Kalkül nehmen müssen:

$$\text{(comm)}\ \frac{\Gamma, \alpha, \beta \vdash \Delta}{\Gamma, \beta, \alpha \vdash \Delta.} \qquad \frac{\Gamma \vdash \Delta, \alpha, \beta}{\Gamma \vdash \Delta, \beta, \alpha.}$$

$$\text{(contr)}\ \frac{\Gamma, \alpha, \alpha \vdash \Delta}{\Gamma, \alpha \vdash \Delta} \qquad \frac{\Gamma \vdash \Delta, \alpha, \alpha}{\Gamma \vdash \Delta, \alpha}$$

Man sagt, diese Regeln sind **zulässig**, sie fügen dem Kalkül nichts hinzu. Der Grund hierfür ist, dass – wenn wir die Notation auf ihre eigentliche Bedeutung zurückführen – sich von Anzezedent zu Konsequent der Regeln nichts ändert.

Ein **formaler Beweis** ist ein Baum in dem

- jedes Blatt eine Instanz von (ax) ist;
- Jeder innere Knoten eine Instanz einer Regel des Kalküls CL ist.

Wir schreiben:

$$\Vdash_{\mathsf{CL}} \Gamma \vdash \Delta,$$

falls es einen formalen Beweis gibt, an dessen Wurzel $\Gamma \vdash \Delta$ steht.

10.3 Die "Bedeutung" von Sequenten

Die Essenz der Beweistheorie ist, das Beweise rein syntaktische Objekte sind, die keine Interpretation brauchen. Um die Regeln intuitiv nachvollziehen zu können, ist es aber dennoch sinnvoll, zu verstehen was ein Sequent bedeutet. Nehmen wir den Sequenten

$$\Gamma \vdash \alpha,$$

wobei

$$\Gamma = \{\gamma_1, \gamma_2 ..., \gamma_n\}$$

Dann bedeutet der obige Sequent soviel wie:

$$\text{Aus } \gamma_1 \text{ und } \gamma_2 \text{ und ... und } \gamma_n \text{ folgt } \alpha.$$

Nun nehmen wir einen Sequenten

$$\Gamma \vdash \Delta,$$

wobei

$$\Delta = \{\delta_1, \delta_2, ..., \delta_m\}$$

Das bedeutet soviel wie:

$$\begin{array}{ll} & \text{Aus } \gamma_1 \text{ und } \gamma_2 \text{ und ... und } \gamma_n \text{ folgt } \delta_1, \\ \text{oder:} & \text{aus } \gamma_1 \text{ und } \gamma_2 \text{ und ... und } \gamma_n \text{ folgt } \delta_2, \\ & \vdots \\ \text{oder:} & \text{aus } \gamma_1 \text{ und } \gamma_2 \text{ und ... und } \gamma_n \text{ folgt } \delta_m. \end{array}$$

Das bedeutet:

- links des '$\vdash$' bedeutet Mengen (bzw. das Komma) **Konjunktion**, formaler: $\Gamma \cong \bigwedge \Gamma$;
- rechts des '$\vdash$' bedeutet Mengen (bzw. das Komma) **Disjunktion**, formaler: $\Gamma \cong \bigvee \Gamma$;

Hier bedeuten

$$\begin{array}{l} \bigwedge\{\gamma_1, ..., \gamma_n\} = \gamma_1 \wedge ... \wedge \gamma_n; \\ \bigvee\{\gamma_1, ..., \gamma_n\} = \gamma_1 \vee ... \vee \gamma_n. \end{array}$$

Die Korrespondenz lässt sich natürlich auch sehr einfach an den Regeln ($\wedge$I),(I$\vee$) ablesen.

10.4 Entscheidbarkeit und Schnitt

Dieser Kalkül hat eine wunderbare Eigenschaft: für jede Regel (mit einer Ausnahme), die wir anwenden, wird der Sequent der daraus entsteht in einem gewissen Sinne **komplexer** als seine Vorgänger. Das bedeutet: wir können effektiv entscheiden, ob ein Sequent beweisbar ist, denn der Suchraum für mögliche Vorgänger ist endlich.

Die eine Ausnahme ist die Regel (schnitt), die in etwa der logischen Transitivität entspricht; diese Regel hat daher in der Geschichte der Logik immer besondere Aufmerksamkeit bekommen – insbesondere die Frage, ob man sie aus formalen Beweisen **eliminieren** kann. Das ist möglich, wie wir später sehen werden. Daraus folgt dann bereits die Entscheidbarkeit des Kalküls.

Dennoch hier eine wichtige Einschränkung: aus der Tatsache, dass wir einen Beweis "vor die Wand fahren", also nicht auf Axiome zurückführen können, folgt erstmal nichts! Insbesondere zeigt das nicht, das ein Sequent nicht beweisbar ist! Um das zu zeigen, ist es nötig zu zeigen, dass es keinen Beweis gibt. Beweisregeln sind aber, wenn man von unten nach oben sucht, zum Teil hochgradig nicht-deterministisch. Insofern ist der Gentzen Kalkül keine gute Methode, um zu beweisen dass ein Sequent falsch ist!

Übung 5

Beweisen Sie folgende Sequenten:

1. $\neg p \wedge \neg q \vdash \neg(p \vee q)$
2. $\neg(p \vee q) \vdash \neg p \wedge \neg q$
3. $(p \to q) \wedge p \vdash q$
4. $(p \to q) \to p \vdash p \to (q \to p)$
5. $(p \to q) \to r \vdash p \to (q \to r)$
6. $(p \vee q) \to r \vdash (p \to r) \wedge (q \to r)$
7. $(p \to r) \wedge (q \to r) \vdash (p \vee q) \to r$
8. $\vdash (p \to (p \to q)) \vee p$
9. $p \vee (q \wedge r) \vdash (p \vee r) \wedge (p \vee q)$
10. $(p \vee r) \wedge (p \vee q) \vdash p \vee (q \wedge r)$

Übung 6

Beweisen Sie folgenden Sequenten (etwas haarig, aber lehrreich):

$$\vdash ((p \to q) \to p) \to p$$

Lösung: 2. ist etwas schwierig, und wir sehen hier: die Regel $(\to I)$ ist nicht so formuliert, dass wir ohne Schnitt arbeiten können. Der Beweis der Formel braucht tatsächlich eine Instanz von Schnitt. Die Formel ist übrigens bekannt als Peirces Theorem, und ist äquivalent zum Satz des ausgeschlossenen Dritten. Hier der Beweis:

$$\dfrac{\dfrac{\dfrac{\dfrac{p \vdash p}{\vdash p, \neg p}}{(p \to q) \to p \vdash p, \neg p}\,(weak) \qquad \dfrac{p \vdash p \qquad \dfrac{\dfrac{\dfrac{p \vdash p}{p \vdash p, q}}{\neg p, p \vdash q}\,(\neg I)}{\neg p \vdash p \to q}\,(I \to)}{\neg p, (p \to q) \to p \vdash p}}{(p \to q) \to p, (p \to q) \to p \vdash p, p}\,(\textbf{schnitt})}{((p \to q) \to p) \vdash p}\,(\text{notation})}{\vdash ((p \to q) \to p) \to p}\,(I \to)$$

Man sieht hier die Applikation von Schnitt, welche die Formel $\neg p$ eliminiert (man nennt das die **Schnittformel**). Man bemerkt, wenn man den Beweis sucht, auch gleich das Problem: es gibt erstmal keinen syntaktischen Anhaltspunkt, welches die Schnittformel ist. Man muss also wirklich nachdenken!

Diesen Beweis kann man nicht mit unseren Regeln ohne Schnitt durchführen. Wir sehen hier auch, worum es bei Beweistheorie geht: nämlich die Regeln so zu formulieren, dass Schnitt zulässig bleibt. Wir haben ($\to$I) nicht allgemein genug formuliert. Die richtige Formulierung wäre:

$$(\to\mathrm{I})\ \frac{\Gamma, \alpha \vdash \Delta \quad \Theta \vdash \beta, \Delta}{\Gamma, \Theta, \beta \to \alpha \vdash \Delta}$$

Ich habe dieses zweite Δ weggelassen um die Regel übersichtlicher zu machen - zu Unrecht, wie man sieht. Nun wird der Beweis einfacher:

$$\dfrac{\dfrac{p \vdash p \quad \dfrac{\dfrac{p \vdash p}{p \vdash q, p}\ \text{weak}}{\vdash p \to q, p}\ (I \to)}{((p \to q) \to p) \vdash p}\ (\to I)}{\vdash ((p \to q) \to p) \to p}\ (I \to)$$

Und noch Übungen...

- $(p \to \neg p) \vdash \neg p$
- $(p \vee q) \wedge \neg p \vdash q$
- $(p \vee q) \to r \vdash p \to r$

11 Die wichtigsten Ergebnisse in Kürze

11.1 Substitutionen

Eine wichtige Rolle in der Logik spielen Substitutionen. Eine Substitution ist eine Abbildung

$$\sigma : \mathit{Var} \to \mathtt{WFF}$$

die *kanonisch* erweitert wird auf Formeln durch

- $\sigma(\alpha \wedge \beta) = \sigma(\alpha) \wedge \sigma(\beta)$
- $\sigma(\alpha \vee \beta) = \sigma(\alpha) \vee \sigma(\beta)$
- $\sigma(\alpha \to \beta) = \sigma(\alpha) \to \sigma(\beta)$
- $\sigma(\neg(\alpha) = \neg(\sigma(\alpha))$

Wichtig ist hier das folgende Ergebnis:

Lemma 6 *Falls* $\Vdash_{\mathsf{CL}} \Gamma \vdash \Delta$*, dann* $\Vdash_{\mathsf{CL}} \sigma[\Gamma] \vdash \sigma[\Delta]$

Das bedeutet: logische Konsequenz ist geschlossen unter Substitution. Wie beweist man das? Wir zeigen dass gilt

(22) $\Vdash_{\mathsf{CL}} \alpha \vdash \alpha$ für alle $\alpha \in \mathtt{WFF}$.

Das macht man mit einer **Induktion über die Komplexität von** α, d.h. die Anzahl der Konnektoren.

Nun können wir, im Beweis von $\Gamma \vdash \Delta$ einfach alle atomaren Propositionen substitutieren; d.h. unsere Blätter werden die Form haben

$$\overline{\sigma(p) \vdash \sigma(p)}$$

Das ist wegen (22) beweisbar, also können wir einen neuen Beweis konstruieren.

11.2 Konsistenz, Maximalkonsistenz

Ein Kalkül ist **inkonsistent**, falls wir darin einen Widerspruch ableiten können, z.B. $\vdash p \wedge \neg p$. Es ist nicht schwer zu sehen, dass man mit (schnitt) dann *jede* Formel ein Theorem ist: denn dann haben wir

$$\text{(23)} \quad \dfrac{\vdash p \wedge \neg p \qquad \dfrac{p \wedge \neg p \vdash}{p \wedge \neg p \vdash \alpha}\,(weak)}{\vdash \alpha}\,(schnitt)$$

Das bedeutet: wir können auch einfach sagen, ein Kalkül ist inkonsistent falls jede Formel ein Theorem ist.

Umgekehrt, wenn wir Schnitt eliminieren können, dann ist es relativ leicht zu zeigen, dass unser Kalkül konsistent ist: denn wenn er inkonsistent wäre, dann könnten wir

$$\vdash p \wedge \neg p$$

beweisen – aber wie soll der schnittfreie Beweis aussehen? Mit (schnitt) funktioniert dieses Argument natürlich nicht mehr.

Es gibt noch eine weitere interessante Eigenschaft von CL. Wir setze

(24) $\mathsf{Th}_{\mathsf{CL}} = \{\alpha : \vdash \alpha \text{ ist beweisbar in } \mathsf{CL}\}$

Wir sagen nun: eine **Theorie** ist eine Menge von Formeln, die geschlossen ist unter $\vdash$:

(25) $\mathsf{Th}_{\mathsf{CL}}(\Gamma) = \{\alpha : \Gamma \vdash \alpha \text{ ist beweisbar in } \mathsf{CL}\}$

Natürlich gilt:

(26) $\Gamma \subseteq \mathsf{Th}_{\mathsf{CL}}(\Gamma)$

Weiterhin:

Definition 7 *Eine Menge Γ ist geschlossen unter Substitution, falls für jede Substitution σ gilt: falls $\alpha \in \Gamma$, dann ist $\sigma(\alpha) \in \Gamma$.*

Maximalkonsistenz bedeutet soviel wie:

Lemma 8 *Nimm an,* Γ *ist geschlossen unter Substitution. Dann gilt:*

1. *Entweder,* $\Gamma \subseteq \mathsf{Th}_{\mathsf{CL}}$*,*

2. *oder* $\mathsf{Th}_{\mathsf{CL}}(\Gamma) = \mathtt{WFF}$*, d.h. die Theorie ist inkonsistent.*

In diesem Sinne ist CL maximal: es gibt viele schwächere Logiken, aber keine stärkere. Anders gesagt: der Versuch, CL mit einer zusätzlichen Beweisregel auszustatten, ist immer zur Folge, dass der Kalkül inkonsistent wird.

11.3 Schnitt-Eliminierung

Hier nur eine kurze Einführung in die Schnitt-Eliminierung: man eliminiert Schnitt, indem man ihn im Beweis *nach oben* verschiebt.

11.4 Vollständigkeit

Der Vollständigkeitssatz für die Aussagenlogik sagt folgendes:

Satz 9 *$\alpha \models \beta$ genau dann wenn $\Vdash_{\mathsf{CL}} \alpha \vdash \beta$.*

Das bedeutet, die syntaktische und die semantische Konsequenz fallen zusammen!

$\Leftarrow$ Induktion über die Regel: die Prämisse (d.i. die Oberseite) ist korrekt, also auch die Konsequenz (d.i. die Unterseite).

$\Rightarrow$ Beweisen kann man das mit Booleschen Algebren: wir schreiben $\alpha \dashv\vdash \beta$ bedeutet, dass $\alpha \vdash \beta$, $\beta \vdash \alpha$. Wir können nun **Äquivalenzklassen** definieren:

$$\alpha_{\dashv\vdash} = \{\beta : \alpha \dashv\vdash \beta\}.$$

Zuletzt definieren wir die Menge aller Äquivalenzklassen von Formeln:

$$\mathtt{WFF}_{\dashv\vdash} = \{\alpha_{\dashv\vdash} : \alpha \in \mathtt{WFF}\}$$

Diese Menge bildet eine Boolesche Algebra: wir definieren

- $M \cup N = (\alpha \vee \beta)_{\dashv\vdash}$ für ein beliebiges $\alpha \in M, \beta \in N$,
- $M \cap N = (\alpha \wedge \beta)_{\dashv\vdash}$ für ein beliebiges $\alpha \in M, \beta \in N$,
- $\overline{M} = (\neg\alpha)_{\dashv\vdash}$ für ein beliebiges $\alpha \in M, \beta \in N$
- $1 = (p \vee \neg p)_{\dashv\vdash}$ für ein beliebiges p
- $0 = (p \wedge \neg p)_{\dashv\vdash}$ für ein beliebiges p

Die Formelalgebra $(\mathtt{WFF}_{\dashv\vdash}, \cap, \cup, \overline{[-]}, 0, 1)$ ist tatsächlich eine Boolesche Algebra. Es ist eine sehr sinnvolle und interessante Übung zu zeigen, dass diese Algebra mit den Operationen, so wie oben definiert, tatsächlich eine Boolesche Algebra ist.

Kleines Quiz zur Aussagenlogik

1. Was ist eine Logik?
2. Gibt es noch andere Logiken?
3. Was ist eine induktive Definition, und warum ist das so wichtig in der Logik (mind 2 Gründe)?
4. Was ist eine Semantik, und was soll sie tun?
5. Warum gibt es Beweistheorie? (mind. 2 Gründe)
6. Was bedeutet Maximalkonsistenz?
7. Was ist Vollständigkeit?
8. Warum ist Schnitt so problematisch?

Und nun die große Fragen die uns weiterführen:

1. Warum ist Aussagenlogik so unbefriedigend?
2. Wie können wir dafür Abhilfe schaffen?

12 Prädikatenlogik – Syntax

Die Zutaten für die Sprache der Prädikatenlogik sind folgende:

1. die propositionalen Konnektoren $\wedge, \vee, \neg, \rightarrow$
2. eine (abzählbar unendliche) Menge von Variablen $Var = \{x_1, x_2, x_3, ...\}$; wir schreiben oft auch x, y, z etc.

Wir brauchen aber noch mehr, nämlich die Quantoren:

3. die Quantoren $\forall, \exists$, der sog. Allquantor und Existenzquantor

Zuletzt kommen noch die Prädikate (und Funktionen und Konstanten). Die sind aber nicht allgemein festgelegt, sondern müssen konkret für eine Sprache bestimmt werden. Deswegen definieren wir ein **Vokabular** V wie folgt:

Ein Vokabular ist ein Paar

$$V = (\Omega, (P_1, ..., P_m, f_1, ..., f_n, a_1, ..., a_o)),$$

wobei

- $P_1, ..., P_m$ die **Prädikate** sind, und $\Omega(P_i)$ für jedes Prädikat die **Arität** festlegt (die Anzahl der Argumente).
- $f_1, ..., f_n$ die **Funktionen** sind, und $\Omega(P_i)$ für jede Funktion die **Arität** festlegt.
- $a_1, ..., a_o$ sind die **Konstanten**.

Eigentlich ist diese Definition vereinfacht, denn alle diese Mengen von Prädikaten / Funktionen / Konstanten können durchaus auch unendlich sein. Wir werden noch eine Vereinfachung vornehmen: Funktionen bleiben erstmal außen vor, d.h. wir werden sie bis auf weiteres nicht nutzen (das macht folgende Definitionen einfacher). Wir haben nun weitere Zutaten:

4. Ein Vokabular V;
5. Ein Gleichheitssymbol '$\doteq$' gibts auch immer.

Und damit sind wir fertig, d.h. wir können nun die **wohlgeformten Formeln** `WFF` definieren:

- Jedes $x \in \mathit{Var}$ ist ein wohlgeformter Term.
- Jede Konstante a in V ist ein wohlgeformter Term.
- Falls $t_1, ..., t_n$ wohlgeformte Terme sind, f ein Funktionssymbol mit $\Omega(f) = n$, dann ist $f(t_1, ..., t_n)$ ein wohlgeformter Term.

Zu Formeln kommen wir in einem einfachen Schritt:

- Falls $t_1, ..., t_n$ wohlgeformte Terme sind, $\Omega(P) = n$, dann ist $P(t_1, ..., t_n)$ eine wohlgeformte Formel.
- Falls t_1, t_2 wohlgeformte Terme sind, dann ist $t_1 \doteq t_2$ eine wohlgeformte Formel.
- Falls α, β wohlgeformte Formeln sind, dann sind $\alpha \wedge \beta$, $\alpha \vee \beta$, $\alpha \rightarrow \beta$, $\neg\alpha$ wohlgeformte Formeln.
- Falls α eine wohlgeformte Formel ist, $x \in \mathit{Var}$ dann sind $\forall x.\alpha$, $\exists x.\alpha$ wohlgeformte Formeln.
- Sonst ist nichts eine wohlgeformte Formel!

Eine besondere Bedeutung kommt denn sog. **geschlossenen Formeln** zu. Wir definieren die freien Variablen einer Formel wie folgt (induktiv wie immer):

- $FV(x) = \{x\}$, für $x \in \mathit{Var}$.
- $FV(a) = \emptyset$, für a eine Konstante.
- $FV(f(t_1, ..., t_n)) = FV(t_1) \cup ... \cup FV(t_n)$
- $FV(P(t_1, ..., t_n)) = FV(t_1) \cup ... \cup FV(t_n)$.
- $FV(\alpha \vee \beta) = FV(\alpha \wedge \beta) = FV(\alpha \rightarrow \beta) = FV(\alpha) \cup FV(\beta)$
- $FV(\neg(\alpha)) = FV(\alpha)$
- $FV(\exists x.\alpha) = FV(\forall x.\alpha) = FV(\alpha) - \{x\}$

Das bedeutet: Variablen, über die quantifiziert wird, sind nicht mehr frei.

Definition 10 *Eine Formel α ist **geschlossen**, wenn $FV(\alpha) = \emptyset$.*

13 Prädikatenlogik – Semantik

Wir definieren jetzt die Semantik dieser Sprache. Wichtig: bevor wir ein Modell definieren können, müssen wir ebenfalls das Vokabular festlegen; das ist in der Prädikatenlogik immer das erste! Einfachheit halber nehmen wir an, dass unser Vokabular keine Funktionen hat, also die Form hat

$$V = (\Omega, (P_1, ..., P_n, a_1, ..., a_m))$$

Wir haben also Prädikate und Konstanten. Wir denotieren die Menge der Konstanten $a_1, ..., a_m$ mit *konst*. Wir definieren ein Modell für dieses Vokabular als ein Tupel

$$\mathcal{M} = (U, R_1, ..., R_n, \overline{a}_1, ..., \overline{a}_m)$$

wobei

1. U das Universum ist, also die Menge der Individuen;
2. $\overline{a}_1, ..., \overline{a}_n \in U$ sind Individuen;
3. für alle $i : 1 \leq i \leq n$ gilt: $R_i \subseteq U^{\Omega(P_i)}$

3. bedeutet also soviel wie: wenn P_i ein n-äres Prädikat ist (rein syntaktisch), dann ist R_i eine n-äre Relation, n eine beliebige natürlich Zahl. Es gibt also eine 1 zu 1 Relation sowohl

- zwischen Prädikaten und Relationen, die natürlich die Stelligkeit präservieren muss;
- und Konstantent a_i und Individuen $\overline{a}_i$.

Ebenso wichtig wie diese Relation ist aber auch die Tatsache, dass die Objekte ontologisch verschieden sind: a_i ist eine Konstante, ein Symbol unserer Sprache; $\overline{a}_i$ ist ein konkretes Objekt unseres Universums, das von a_i denotiert wird.

Wir haben nun Modelle; was wir als nächstes definieren, ist die Erfüllungsrelation $\models$. Das geht aber nicht so einfach, denn zwar sind geschlossene Formeln wahr oder falsch, aber offene Formeln nicht, da die Bedeutung von Variablen erstmal nicht festgelegt ist. Dennoch müssen wir auch diesen Formeln eine Bedeutung geben, denn wie sollten wir eine induktiv definierte Bedeutung von

$$\exists x.\alpha$$

festlegen, ohne eine Bedeutung von α zu haben – wobei α möglicherweise eine offene Formel ist? Die Lösung dieses Problem liegt in der Annahme von **Belegungsfunktionen** (oder kurz Belegung). Um die folgenden Definitionen etwas eleganter zu gestalten, nehmen wir einfach an, dass eine Belegung eine Funktion ist

$$\sigma : \mathit{Var} \cup \mathit{konst} \to U$$

also Variablen und Konstanten werden als Individuen des Universums interpretiert. Dabei ist die Interpretation von *konst* festgelegt:

$$\text{für alle } a_i \in \mathit{konst} \text{ gilt: } \sigma(a_i) = \overline{a}_i$$

für Variablen $x \in \mathit{Var}$ ist der Wert $\sigma(x)$ beliebig, dementsprechend gibt viele verschiedene Belegungen. Es gibt eine wichtige Relation zwischen Belegungen: wir schreiben, für zwei Belegungen σ, σ'

$$\sigma \sim_x \sigma', \text{ falls für alle } y \in \mathit{Var} - \{x\} \text{ gilt: } \sigma(y) = \sigma'(y)$$

Das bedeutet also: die Belegungen unterscheiden sich nur darin, wie sie x belegen, sonst in nichts. Nun können wir die **Wahrheit** einer Formel definieren, allerdings nicht im Hinblick auf ein Modell, sondern ein Modell *und* eine Belegung.

Nimm also ein Vokabular, ein Modell und eine Belegung als gegeben. Dann gilt:

$M, \sigma \models P_i(t_1, ..., t_n)$ genau dann wenn $(\sigma(t_1), ..., \sigma(t_n)) \in R_i$.

$M, \sigma \models t_1 \doteq t_2$ gdw. $\sigma(t_1) = \sigma(t_2)$

$M, \sigma \models \alpha \wedge \beta$, gdw. $M \models \alpha$ und $M \models \beta$.

$M, \sigma \models \alpha \vee \beta$, gdw. mindestens eines der beiden gilt, $M \models \alpha$ oder $M \models \beta$.

$M, \sigma \models \neg\alpha$, gdw. $M \not\models \alpha$

$M, \sigma \models \alpha \to \beta$, gdw. mindestens eines der beiden gilt, $M \not\models \alpha$ oder $M \models \beta$.

$M, \sigma \models \exists x.\alpha$, gdw. gilt: es gibt ein σ' so dass 1. $\sigma \sim_x \sigma'$, und 2. $M, \sigma' \models \alpha$

$M, \sigma \models \forall x.\alpha$, gdw. gilt: für alle σ', falls $\sigma \sim_x \sigma'$, dann $M, \sigma' \models \alpha$.

Die Definitionen der Konnektoren sind wie gehabt; zu beachten ist:

- In der ersten Klausel wird gesagt, dass das Prädikat als die korrespondierende Relation interpretiert wird, und das Prädikat ist wahr auf seine Argumente bezogen, wenn deren Belgung (als Tupel) In der Relation enthalten sind.
- In der zweiten Klausel wird gesagt, dass das Symbol $\doteq$ als Gleichheit im Modell interpretiert wird, also $t_1 \doteq t_2$ ist wahr gdw. t_1 und t_2 als das gleiche identische Objekt denotiert werden.
- Die Interpretation der Quantoren besagt: für $\exists x.\alpha$ muss es eine Belegung geben, deren Wert sich nur in x unterscheidet, die α wahr macht; und
- für $\forall x.\alpha$ muss jede Belegung, die sich nur in x unterscheidet, α wahr machen. Das fällt mit unserem intuitiven Begriff von Quantifikation zusammen.

Die ersten zentralen Ergebnisse dieser Semantik sind die folgenden:

Lemma 11 *Nimm an, $x \notin FV(\alpha)$, und $\mathcal{M}, \sigma \models \alpha$. Dann gilt für alle σ': falls $\sigma \sim_x \sigma'$, dann $\mathcal{M}, \sigma' \models \alpha$.*

Das bedeutet: die Belegung von nicht-freien Variablen spielt keine Rolle. Der Beweis dieses Lemmas ist wie üblich eine Induktion über Formelkomplexität: wir zeigen dass es für atomare Formeln gilt, sich über Konnektoren bewahrt. Der kritische Fall ist, zu zeigen dass es auch für $\exists x.\alpha$ und $\forall x.\alpha$ gilt, wenn $x \in FV(\alpha)$.

Dieses Lemma hat nun eine wichtige Konsequenz, die als ein Spezialfall daraus folgt:

Lemma 12 *Nimm an, α ist eine geschlossene Formel. Dann gilt $\mathcal{M}, \sigma \models \alpha$ genau dann wenn für alle σ' gilt $\mathcal{M}, \sigma' \models \alpha$.*

Das bedeutet: ob α in einem Modell $\mathcal{M}$ wahr ist, ist *unabhängig* von σ, und wir können daher (für geschlossene Formeln) schreiben:

$$\mathcal{M} \models \alpha$$

Also haben wir Formeln, die in Modellen wahr oder falsch sind. Dementsprechend können wir den Begriff der Tautologie, der Implikation etc. aus der Aussagenlogik übernehmen, und schreiben:

$$\alpha \models \beta, \models \alpha \text{ etc.}$$

Beispiele Wir definieren eine Reihe von Modellen:

- $\mathcal{M}_1 := (\{\overline{h}, \overline{g}, \overline{k}\}, R_l = \{(\overline{h}, \overline{g}), (\overline{g}, \overline{k}), (\overline{k}, \overline{k})\})$
- $\mathcal{M}_2 := (\{\overline{h}, \overline{g}, \overline{k}, \overline{p}\}, R_l = \{(\overline{h}, \overline{g}), (\overline{g}, \overline{k}), (\overline{k}, \overline{k})\})$
- $\mathcal{M}_3 := (\{\overline{h}, \overline{g}, \overline{k}, \overline{p}\}, R_l = \{(\overline{h}, \overline{g}), (\overline{g}, \overline{k}), (\overline{k}, \overline{k}), (\overline{k}, \overline{p}), (\overline{p}, \overline{h})\})$
- $\mathcal{M}_4 := (\{\overline{h}, \overline{g}, \overline{k}\}, R_l = \{(\overline{h}, \overline{g}), (\overline{g}, \overline{h}), (\overline{k}, \overline{h})\})$
- $\mathcal{M}_5 := (\{\overline{h}, \overline{g}, \overline{k}\}, R_l = \{(\overline{h}, \overline{g}), (\overline{g}, \overline{k}), (\overline{k}, \overline{h})\})$
- $\mathcal{M}_6 := (\{\overline{h}, \overline{g}\}, R_l = \{(\overline{h}, \overline{h}), (\overline{h}, \overline{g}), (\overline{g}, \overline{g}), (\overline{g}, \overline{h})\})$

Und dazu eine Reihe von Formeln:

- $\alpha_1 := \forall x.\exists y.l(x, y)$
- $\alpha_2 := \exists y.\forall x.l(x, y)$
- $\alpha_3 := \forall xy.l(x, y) \vee l(y, x)$
- $\alpha_3' := \forall xy.l(x, y) \vee l(y, x) \vee x \doteq y$
- $\alpha_4 := \forall xy.l(x, y) \rightarrow (\neg l(y, x))$
- $\alpha_5 := \exists x.\neg\forall y.l(x, y)$
- $\alpha_6 := \forall xyz.(l(x, y) \wedge l(x, z)) \rightarrow y \doteq z$
- $\alpha_7 := \forall xyz.(l(x, z) \wedge l(y, z)) \rightarrow x \doteq y$

Antworten (teilweise) $\mathcal{M}_1 \models \alpha_1$? Wahr!

$\mathcal{M}_2 \models \alpha_1$? Falsch!

$\mathcal{M}_1 \models \alpha_2$? Falsch!

$\mathcal{M}_3 \models \alpha_1$? Wahr!

$\mathcal{M}_1 \models \alpha_3$? Falsch! (zwischen k, h gibt es kein l)

$\mathcal{M}_3 \models \alpha_3$? Falsch!

$\mathcal{M}_1 \models \alpha_4$? Falsch, (k, k)!

$\mathcal{M}_4 \models \alpha_4$? Falsch, (g, h) und (h, g)!

$\mathcal{M}_5 \models \alpha_4$? Wahr!

$\mathcal{M}_5 \models \alpha_3$? Wahr!

$\mathcal{M}_5 \models \alpha_5$? Wahr! Sie müssen ein x finden so dass $\forall y.l(x, y)$ falsch wird – dass gilt für jedes x!

$\mathcal{M}_6 \models \alpha_5$? Falsch, alle lieben alle!

$\mathcal{M}_5 \models \alpha_6$? Korrekt. Das bedeutet: Funktionalität: $l(x) = y$ könnte man schreiben.

$\mathcal{M}_6 \models \alpha_6$? Falsch, $(h, h), (h, g)$ und $g \neq h$

$\mathcal{M}_5$ ist das einzige Modell, das α_7 erfüllt.

Hausaufgabe zum 13.12.21

Prüfen Sie die Wahrheit von α_1 bis α_5 in $\mathcal{M}_4$! (α_4 steht bereits oben).

Übung 7

Nehmen Sie folgende Formeln:

1. $\alpha_8 := \forall xy.[(l(x,y) \wedge l(y,x)) \rightarrow x \doteq y]$
2. $\alpha_9 := \forall xy.[l(x,y) \vee \exists z.(l(x,z) \wedge l(z,y))]$
3. $\alpha_{10} := \exists x.\forall yz.[(l(x,y) \wedge l(y,z)) \rightarrow l(x,z)]$

Gehen Sie durch die Liste $\mathcal{M}_1 - \mathcal{M}_6$ und schreiben Sie für jede Formel, in welchen Modellen sie wahr ist.

14 Wahrheit und Konsequenz in Prädikatenlogik

14.1 Die Frage nach der Wahrheit im Modell

Die Frage, ob $M \models \alpha$, ist bei endlichen Modellen M (also $|U| < \infty$) mechanisch entscheidbar: wir müssen nur, je nach Quantor, durch die Belegungen gehen. Falls das Modell sehr groß ist, kann das aber trotzdem zu Problemen führen: nimm an dass

- $|U| = 10^6$, und
- $\alpha = \forall x_1.\exists x_2.\forall x_3.\exists x_4.\alpha'$

In diesem Fall ist das Problem praktisch nicht mehr lösbar mit roher Gewalt, und wir müssen uns etwas einfallen lassen!

14.2 Semantische Konsequenz

Wir hatten die Relation $\alpha \models \beta$ definiert für Aussagenlogik; wir tun nun dasselbe für Prädikatenlogik. Man kann das machen sowohl für offene also auch geschlossene Formeln:

Definition 13 *$\alpha \models \beta$ gdw. für alle M, σ gilt: falls $M, \sigma \models \alpha$, dann $M, \sigma \models \beta$. Wir schreiben $\models \alpha$ gdw. $M, \sigma \models \alpha$ für alle M und σ.*

Falls α, β geschlossen sind, ist σ irrelevant, und das ganze vereinfacht sich zu $\alpha \models \beta$ gdw. für alle M gilt: falls $M \models \alpha$, dann $M \models \beta$.

Und das ist nun schwierig: denn die Menge/Klasse Modelle ist unendlich, und es gibt *keinen Weg sie auf endlich viele zu reduzieren*!

$\Rightarrow$ Semantische Konsequenz in Prädikatenlogik zwingt uns, nachzudenken, und das ist immer schlecht!

Hier gibt es nun zwei Möglichkeiten:

1. Wir denken, dass $\alpha \models \beta$ wahr ist. Wir müssen also ein abstraktes Argument über *alle* Modelle machen!
2. Wir denken, dass $\alpha \models \beta$ falsch ist. In diesem Fall müssen wir *ein* Modell konstruieren, in dem α wahr, β falsch ist.

So oder so, das riecht nach Ärger.

Übung 8

Entscheiden Sie, ob folgende Aussagen gültig sind:

1. $\models \forall xyz.(x \doteq y \wedge y \doteq z) \rightarrow x \doteq z$
2. $\models \forall xyz.((P(x,y) \wedge x \doteq z) \rightarrow P(z,y))$
3. $\exists x.\alpha \models \forall x.\alpha$ (α beliebig)
4. $\forall x.\alpha \models \exists x.\alpha$ (α beliebig)
5. $\forall x.\exists y.\alpha \models \exists y.\forall x.\alpha$ (α beliebig)
6. $\exists y.\forall x.\alpha \models \forall x.\exists y.\alpha$ (α beliebig)
7. $\exists x.(P(x) \wedge Q(x)) \models (\exists x.P(x)) \wedge (\exists x.Q(x))$
8. $(\exists x.P(x)) \wedge (\exists x.Q(x)) \models \exists x.(P(x) \wedge Q(x))$
9. $\exists x.(P(x) \vee Q(x)) \models (\exists x.P(x)) \vee (\exists x.Q(x))$
10. $\forall x.P(x) \rightarrow Q(x) \models (\forall(x).P(x)) \rightarrow (\forall y.Q(y))$
11. $\exists x.P(x) \rightarrow Q(x) \models (\exists x.P(x)) \rightarrow (\exists y.Q(y))$

Vorsicht: hier hilft keine formale Prozedur (erstmal), sondern nur ein echtes Argument. Also überlegen!

Hier sind eine Reihe von wichtigen Techniken gefragt:

- Falls wir denken, $\alpha \models \beta$ ist falsch, dann versuchen wir das mit einem Gegenbeispiel zu zeigen; d.h. wir konstruieren ein Modell $\mathcal{M}$ so dass $\mathcal{M} \models \alpha$ aber $\mathcal{M} \not\models \beta$.
- Falls wir denken, $\alpha \models \beta$ ist richtig, dann versuchen wir zu zeigen, dass ein beliebiges Modell, dass α erfüllt, auch β erfüllt.
- Hierbei ist entscheidend: der Schritt von *ein beliebiges Modell* $\mathcal{M}$ das α erfüllt, erfüllt auch β, zu *jedes Modell* $\mathcal{M}$. Das ist legitim, wenn wir keine Annahmen über $\mathcal{M}$ gemacht haben.
- Dasselbe gilt natürlich auch für Belegungen!

Lösungen 1. Richtig: Nimm ein beliebiges Modell mit Belegung $\mathcal{M}, \sigma$. Nimm nun an, $\mathcal{M}, \sigma \models (x = y \wedge y = z)$. Dann gilt: $\sigma(x) = \sigma(y)$ und $\sigma(y) = \sigma(z)$. Also gilt $\mathcal{M}, \sigma \models x = z$. Also gilt (ohne irgendeine Annahme) dass $\mathcal{M}, \sigma \models (x = y \wedge y = z) \to x = z$,

2. Richtig: Nimm an, $\mathcal{M}, \sigma \models P(x, y) \wedge x = z)$. Dann ist $(\sigma(x), \sigma(y)) \in R_P$, und $\sigma(x) = \sigma(z)$; also $(\sigma(z), \sigma(y)) \in R_P$, mithin also $\mathcal{M}, \sigma \models P(z, y)$. Also gilt in jedem Fall (ohne irgendeine Annahme) $\mathcal{M}, \sigma \models (P(x, y) \wedge x = z) \to P(z, y)$ (Argument wie in 1.). Da σ beliebig war, gilt das für jedes σ', also $\mathcal{M}, \sigma \models \forall xyz.(P(x, y) \wedge x = z) \to P(z, y))$. Mit demselben Argument wie in 1. kommt man zu $\models \forall xyz.((P(x, y) \wedge x = z) \to P(z, y))$.

3. Falsch: Wir konstrieren ein Gegenbeispiel, setzen $\alpha \equiv P(x)$, $U \equiv \{a, b\}$, $R_P \equiv \{a\}$ (das ist unser Modell $\mathcal{M}$). Wir zeigen nun: $\mathcal{M} \models \exists x.\alpha$, aber $\mathcal{M} \not\models \forall x.\alpha$. Wir haben ein $\sigma(x) = a$, so dass $\mathcal{M}, \sigma \models P(x)$; also $\mathcal{M} \models \exists x.P(x)$. Allerdings gibt es σ', mit $\sigma'(x) = b$, wobei $\sigma' \sim_x \sigma$. Offensichtlich, $\mathcal{M}, \sigma' \not\models P(x)$, also $\mathcal{M} \not\models \forall x.P(x)$. Also gilt: $\exists x.\alpha \not\models \forall x.\alpha$

4. Falsch, aber nur wegen einem pathologischen Fall, nämlich dem **leeren Modell** $\mathcal{M}_\emptyset$, wobei $U = \emptyset$. Das leere Modell macht jede Aussage $\forall x.\alpha$ wahr, denn für dieses Modell gibt es keine Belegung, also ist die Aussage "für alle σ', ..." immer trivial wahr. Umgekehrt ist jede Formel $\exists x.\alpha$ falsch in $\mathcal{M}_\emptyset$ aus demselben Grund. Das ist aber ein pathologischer Fall, den man oft ausschliesst, denn wen interessieren leere Modelle?

5. Falsch: für jedes Kind gibt es einen Film, den es mag, aber es gibt (je nach Modell) keinen Film den jedes Kind mag. Formal zu zeigen mit Gegenbeispiel: wir setzen $\alpha \equiv P(x, y)$, $U = \{a, b\}$, $R_P = \{(a, b), (b, a)\}$. Wir definieren $\sigma(x) = a, \sigma(y) = b$. Es gilt natürlich $\mathcal{M}, \sigma \models P(x, y)$. Also (da $\sigma \sim_y \sigma$) auch $\mathcal{M}, \sigma \models \exists y.P(x, y)$. Wir zeigen nun, dass für alle σ' gilt: falls $\sigma' \sim_x \sigma$, dann $\mathcal{M}, \sigma' \models \exists y.P(x, y)$. Da es nur zwei Objekte in U gibt, gibt es nur zwei solche Funktionen, nämlich σ selbst, und σ' mit σ' mit $\sigma'(x) = b$. Wir haben bereits gesehen, dass $\mathcal{M}, \sigma \models \exists y.P(x, y)$; wir zeigen dass $\mathcal{M}, \sigma' \models \exists y.P(x, y)$. Dafür brauchen wir ein σ'' so dass 1. $\sigma'' \sim_y \sigma'$

und 2. $\mathcal{M}, \sigma'' \models P(x,y)$. Wir nehmen das σ'', für das gilt: $\sigma''(y) = a$. Offensichtlich gilt dann also $\mathcal{M}, \sigma'' \models P(x,y)$. Damit haben wir gezeigt dass $\mathcal{M}, \sigma \models \forall x.\exists y.P(x,y)$, also (da keine freien Variablen mehr übrig sind) $\mathcal{M} \models \forall x..\exists y.P(x,y)$.

Jetzt kommt Teil 2: nämlich zu zeigen dass $\mathcal{M} \not\models \exists y.\forall x.P(x,y)$. Wir machen das mit einem Widerspruchsbeweis: nimm an, es gilt $\mathcal{M} \models \exists y.\forall x.P(x,y)$. Also gibt es ein σ so dass $\mathcal{M}, \sigma \models \forall x.P(x,y)$. Wir unterscheiden zwei Fälle:

Fall 1 $\sigma(y) = a$ In dem Fall muss gelten: für alle $\sigma' \sim_x \sigma$, $\mathcal{M}, \sigma' \models P(x,y)$. Also auch für σ' mit $\sigma'(x) = a$. Aber da $(a,a) \notin R_P$, gilt $\mathcal{M}, \sigma' \not\models P(x,y)$, also $\mathcal{M}, \sigma \not\models \forall x.P(x,y)$

Fall 2 $\sigma(y) = b$. Das parallele Argument, nur dass wir setzen $\sigma'(x) = b$. Also $\mathcal{M}, \sigma \not\models \forall x.P(x,y)$.

Weil es nur die zwei Möglichkeiten gibt, gilt $\mathcal{M} \not\models \exists y.\forall x.P(x,y)$. Wir haben also ein Modell $\mathcal{M}$ so dass $\mathcal{M} \models \forall x.\exists y.\alpha$, $\mathcal{M} \not\models \exists y.\forall x.\alpha$, also $\forall x.\exists y.\alpha \not\models \exists y.\forall x.\alpha$ (α beliebig)

6. Wir nehmen an, die Domäne U ist *nicht leer* – sonst gilt dasselbe wie in Fall 4 – in dem Fall richtig. Nimm an ein nichtleeres Modell $\mathcal{M}$ erfüllt $\mathcal{M} \models \exists y.\forall x.\alpha$. Das heißt, es gibt ein σ so dass $\mathcal{M}, \sigma \models \forall x.\alpha$, und für alle $\sigma' : \sigma' \sim_x \sigma$ gilt $\mathcal{M}, \sigma' \models \alpha$.

Also gilt (nach Semantik von $\exists$) für alle diese σ', dass $\mathcal{M}, \sigma' \models \exists y.\alpha$. Da nun, wie oben gesagt, das für alle σ' gilt, die $\sigma' \sim_x \sigma$ erfüllen, also nach Semantik von $\forall$, $\mathcal{M}, \sigma' \models \forall x.\exists y.\alpha$, also (da keine freien Variablen) $\mathcal{M} \models \forall x.\exists y.\alpha$.

7. Richtig: nimm an $\mathcal{M} \models \exists x.(P(x) \wedge Q(x))$, also gibt es σ so dass $\mathcal{M}, \sigma \models P(x) \wedge Q(x)$. Nach Semantik von $\wedge$ gilt also: $\mathcal{M}, \sigma \models P(x)$ und $\mathcal{M}, \sigma \models Q(x)$, also $\mathcal{M}, \sigma \models \exists x.P(x)$ und $\mathcal{M}, \sigma \models \exists x.Q(x)$, also $\mathcal{M}, \sigma \models (\exists x.P(x)) \wedge (\exists x.Q(x))$, also $\mathcal{M} \models (\exists x.P(x)) \wedge (\exists x.Q(x))$ (geschlossene Formel).

8. Falsch, wir konstruieren ein Gegenbeispiel: $U = \{a, b\}$, $R_P = \{a\}$, $R_Q = \{b\}$. Es gibt $\sigma(x) = a$, $\sigma'(x) = b$, und $\mathcal{M}, \sigma \models P(x)$, $\mathcal{M}, \sigma' \models Q(x)$, also $\mathcal{M}, \sigma \models \exists x.P(x)$, $\mathcal{M}, \sigma' \models \exists x.Q(x)$. Diese Wahrheit ist aber unabhängig von σ, σ (keine freien Variablen!), also $\mathcal{M} \models (\exists x.P(x)) \wedge (\exists x.Q(x))$. Es gibt aber kein σ so dass $\mathcal{M}, \sigma \models P(x) \wedge Q(x)$ (was soll $\sigma(x)$ sein?), also

$\mathcal{M} \not\models \exists x.P(x) \wedge Q(x)$.

9. Nimm an, $\mathcal{M} \models \exists x.(P(x) \vee Q(x))$. Es gibt also ein σ (Zeuge) so dass $\mathcal{M}, \sigma \models P(x) \vee Q(x)$. Das bedeutet, mindestens eines der beiden ist wahr, entweder $\mathcal{M}, \sigma \models P(x)$, oder $\mathcal{M}, \sigma \models Q(x)$. Wir unterscheiden also Fälle.

Fall 1: $\mathcal{M}, \sigma \models P(x)$. Dann gilt $\mathcal{M}, \sigma \models \exists x.P(x)$, also *a fortiori* $\mathcal{M}, \sigma \models \exists x.P(x) \vee \exists x.Q(x)$, wobei wir σ natürlich weglassen können.

Fall 2: $\mathcal{M}, \sigma \models Q(x)$. Genau parallel.

10. Richtig. Nimm an, $\mathcal{M} \models \forall x.P(x) \to Q(x)$. Das bedeutet: f.a. σ, falls $\sigma(x) \in R_P$, dann $\sigma(x) \in R_Q$. Da $\sigma(x)$ ein beliebiges $a \in U$ sein kann, bedeutet dass soviel wie: $R_P \subseteq R_Q$.

Nimm weiterhin an, $\mathcal{M} \models \forall(x).P(x)$ (ansonsten gilt automatisch $\mathcal{M} \models (\forall(x).P(x)) \to (\forall y.Q(y))$). Das bedeutet: f.a. σ gilt: $\sigma(x) \in R_P$, also $R_P = U$. Da $R_P \subseteq R_Q \subseteq U$, folgt dass $R_Q = U$, also $\mathcal{M} \models \forall y.Q(y)$, also $\mathcal{M} \models (\forall(x).P(x)) \to (\forall y.Q(y))$.

11. Falsch: Nimm das Gegenbeispiel $\mathcal{M} = (\{a, b\}, R_P = \{b\}, R_Q = \emptyset)$. Für $\sigma(x) = a$ gilt $\mathcal{M}, \sigma \models P(x) \to Q(x)$. Aber $\mathcal{M} \models \exists x.P(x)$ (Zeuge: $\sigma(x) = b$), aber $\mathcal{M} \not\models \exists x.Q(x)$ (denn $R_Q = \emptyset$).

Hausaufgabe zum 20.21.21

1. Bearbeiten Sie Teil 3 (also α_{10}) aus Übung 7.

2. Bearbeiten Sie Teil 9,10 aus Übung 8. Falls Sie mit der Formalisierung des Argumentes Probleme haben, machen Sie ein informelles Argument!

15 Interdefinierbarkeit und wichtige Tautologien

Es gibt eine Reihe wichtiger Tautologien in der Prädikatenlogik. Die erste betrifft die Interdefinierbarkeit von $\forall$ und $\exists$:

Lemma 14 *$\mathcal{M} \models \exists x.\alpha$ gdw. $\mathcal{M} \models \neg\forall x.\neg\alpha$ Ebenso: $\mathcal{M} \models \neg\exists x.\neg\alpha$ gdw. $\mathcal{M} \models \forall x.\alpha$.*

Wir können also $\forall$ mit $\exists$ definieren und umgekehrt.

16 Beweistheorie der Prädikatenlogik

Die Beweistheorie für die Prädikatenlogik ist relativ einfach, sie hat nur einen entscheidenden Nachteil: wir haben keine Entscheidbarkeit mehr. Ein sehr wichtiger Begriff ist der der Substitution: sei α eine Formel, t ein Term, x eine Variable. Wir definieren

$$\alpha[t/x],$$

die Substitution von t für x in α, wie folgt:

- $a[t/x] = a$
- $y[t/x] = \begin{cases} y, \text{ falls } y \neq x \\ t \text{ falls } y = x \end{cases}$
- $f(t_1, ..., t_n)[t/x] = f(t_1[t/x], ..., t_n[t/x])$
- $P(t_1, ..., t_n)[t/x] = P(t_1[t/x], ..., t_n[t/x])$
- $(\alpha \star \beta)[t/x] = \alpha[t/x] \star \beta[t/x]$, $\star \in \{\wedge, \vee, \rightarrow\}$
- $(\neg\alpha)[t/x] = \neg(\alpha[t/x])$
- $(\forall y.\alpha)[t/x] = \begin{cases} \forall y.(\alpha[t/x]), \text{ falls } y \neq x \\ \forall y.\alpha \text{ falls } y = x \end{cases}$
- $(\exists y.\alpha)[t/x] = \begin{cases} \exists y.(\alpha[t/x]), \text{ falls } y \neq x \\ \exists y.\alpha \text{ falls } y = x \end{cases}$

Substitution betrifft also freie Variablen! Die Regeln für den Beweiskalkül der Prädikatenlogik sind nun folgende (wir haben ein leicht anderes Axiom und Quantorenregeln; die anderen Regeln aus CL bleiben bestehen!

$$\frac{}{P(t_1, ..., t_n) \vdash P(t_1, ..., t_n)}\ (ax)$$

$$\frac{\alpha[t/x], \Gamma \vdash \Delta}{\forall x.\alpha, \Gamma \vdash \Delta}\ (\forall I) \qquad \frac{\Gamma \vdash \Delta, \alpha[y/x]}{\Gamma \vdash \Delta, \forall x.\alpha}\ (I\forall)$$

$$\frac{\alpha[y/x], \Gamma \vdash \Delta}{\exists x.\alpha, \Gamma \vdash \Delta}\ (\exists I) \qquad \frac{\Gamma \vdash \Delta, \alpha[t/x]}{\Gamma \vdash \Delta, \exists x.\alpha}\ (I\exists)$$

$$\frac{}{\vdash t = t}\ (ax =)$$

$$\frac{\Delta, \alpha \vdash \Gamma}{\Delta, \alpha[t/t'], t = t' \vdash \Gamma}\ (= I) \qquad \frac{\Delta \vdash \Gamma, t = t' \quad \Delta \vdash \Gamma, \alpha[t/t']}{\Delta \vdash \Gamma, \alpha}\ (I =)$$

Das ist aber noch nicht alles, den die Quantorenregeln haben wichtige **Seitenbedingungen**:

$I\forall$ wir verlangen, dass $y \notin FV(\Gamma) \cup FV(\Delta) \cup FV(\forall x.\alpha)$.

$\exists I$ wir verlangen, dass $y \notin FV(\Gamma) \cup FV(\Delta) \cup FV(\exists x.\alpha)$.

Hier fällt wiederum der Parallelismus der Quantorenregeln Regeln auf. Wir können also in diesen Regeln nur über Variablen quantifizieren, wenn *alle* Instanzen dabei gebunden werden. Wohlgemerkt: in diesen Regeln wird gleichzeitig substituiert und quantifiziert. Ebenso: wenn wir Funktionen erlauben, dann führen die Regeln $\forall I$ und $I\exists$ dazu, dass die Länge des Sequenten abnimmt, also der Suchraum unendlich wird! Es gibt noch Regeln für Gleichheit:

Übung 9

Finden Sie formale Beweise für folgende Formeln:

1. $\neg\exists x.P(x) \vdash \forall x.\neg P(x)$
2. $P(x) \wedge \neg P(y) \vdash \neg(x = y)$
3. $\forall xy.x = y \vdash \forall xy.P(x) \to P(y)$
4. $\exists x.\forall y.P(x, y) \vdash \forall y.\exists x.P(x, y)$
5. $\forall xy.(P(x, y) \to Q(y)) \vdash (\forall y.\exists x.P(x, y)) \to (\forall z.Q(z))$
6. $\forall x.\exists y.P(x) \to Q(y) \dashv\vdash (\exists x.P(x)) \to (\exists y.Q(y))$ (Vorsicht, $\dashv$ nicht ohne!)
7. $\forall xy.[\neg(P(x) \to Q(x, y))] \vdash \neg\exists yx.[\neg(P(y) \wedge \neg Q(y, x))]$
8. $\forall xy.[\neg(P(x) \to Q(x, y))] \vdash \neg\exists yx.(\neg P(y) \vee Q(y, x))$
9. $\exists x.\forall y.[Q(x, y) \vee P(x)] \vdash \forall y\exists x.[\neg P(x) \to Q(x, y)]$
10. $(\exists x.P(x)) \to \neg(\forall xy.Q(y, x)) \vdash (\neg\exists xy.\neg Q(x, y)) \to \forall x.\neg P(x)$
11. $\forall xy.(f(x) = f(y)) \to (x = y), f(a) = f(b) \vdash a = b$
12. $\forall xy.(f(x) = f(y)) \to (x = y), f(a) = c, f(b) = c \vdash P(a) \to P(b)$

Eine Musterlösung $(\exists x.P(x)) \to (\exists y.Q(y)) \vdash \forall x.\exists y.P(x) \to Q(y)$

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{Q(y), P(x) \vdash Q(y)}}{Q(y) \vdash P(x) \to Q(y)}\,I\to}{Q(y) \vdash \exists y.P(x) \to Q(y)}\,I\exists}{\exists y.Q(y) \vdash \exists y.P(x) \to Q(y)}\,\exists I \qquad \dfrac{\dfrac{\dfrac{\vdots}{P(x) \vdash P(x), Q(x)}}{\vdash P(x), P(x) \to Q(y)}\,I\to}{\vdash \exists x.P(x), \exists y.P(x) \to Q(y)}\,I\exists \times 2}{(\exists x.P(x)) \to (\exists y.Q(y)) \vdash \exists y.P(x) \to Q(y)}\,\to I}{(\exists x.P(x)) \to (\exists y.Q(y)) \vdash \forall x.\exists y.P(x) \to Q(y)}\,I\forall
$$

Weitere Übungen

Ich nutze hier Prädikate der Form $\leq, <$ mit der üblichen Schreibweise; dabei handelt es sich aber für unsere Beweistheorie um ganz normale Prädikate!

1. $\forall xy.(x \leq y \vee y \leq x) \vdash \forall xy.((\neg x \leq y) \to y \leq x)$
2. $\forall x.x \leq x \vdash \forall x.\exists y.x \leq y$
3. $\forall y.((\neg \exists x.y < x) \to P(y)) \vdash (\exists x.P(x)) \vee \forall x.\exists y.x < y$ (Vorsicht, braucht Vollversion von $(\to I)$)

17 Theorien und Modelle, Axiome

Es gibt wichtige Klassen von Strukturen, über die wir mit Prädikatenlogik sprechen können. Wir schauen uns hier einige sehr grundlegende an. Eine **Theorie** Γ ist einfach eine bestimmte Menge von Formeln (endlich oder unendlich). Wir schreiben

$$\mathcal{M} \models \Gamma \iff \mathcal{M} \models \gamma\text{: für alle } \gamma \in \Gamma$$

Die Klasse der Modelle einer Menge von Formeln ist definiert als

(27) $\mathsf{Mod}(\Gamma) := \{\mathcal{M} : \mathcal{M} \models \Gamma\}$

Umgekehrt, wenn wir eine **Klasse $\mathfrak{C}$ von Modellen** haben (für dasselbe Vokabular), schreiben wir

$$\mathfrak{C} \models \alpha \iff \mathcal{M} \models \alpha\text{: für alle } \mathcal{M} \in \mathfrak{C}$$

Wir defninieren die **Theorie von $\mathfrak{C}$** mittels

(28) $\mathsf{Th}(\mathfrak{C}) = \{\alpha : \mathfrak{C} \models \alpha\}$

Damit bekommen wir nun einen **Hüllenoperator** $\mathsf{Th}\circ\mathsf{Mod}$ (Komposition von Funktionen):

1. $\Gamma \subseteq \mathsf{Th} \circ \mathsf{Mod}(\Gamma)$
2. $\mathsf{Th} \circ \mathsf{Mod}(\Gamma) = \mathsf{Th} \circ \mathsf{Mod}(\mathsf{Th} \circ \mathsf{Mod}(\Gamma))$
3. $\Gamma \subseteq \Delta \Rightarrow \mathsf{Th} \circ \mathsf{Mod}(\Gamma) \subseteq \mathsf{Th} \circ \mathsf{Mod}(\Delta)$

Wenn wir die Relation $\models$ auf Mengen von Formeln erweitern, dann gilt:

(29) $\mathsf{Th} \circ \mathsf{Mod}(\Gamma) = \{\alpha : \Gamma \models \alpha\}$

Man nennt das auch die **deduktive Hülle**: Γ und alles was daraus folgt. Wir können nun also etwas spezifischer sagen:

Definition 15 *Eine* ***Theorie*** *ist eine Menge von Formeln, die abgeschlossen ist unter Inferenz* $\models$.

- $\Rightarrow$ Logiker interessieren sich sehr für Theorien, allerdings sind Theorien immer unendlich (warum?).
- $\Rightarrow$ Statt Theorien schreiben wir also gewöhnlich nur die **Axiome** hin:

Definition 16 *Eine (endliche) Menge* Δ

1. ***axiomatisiert*** *eine* ***Klasse*** $\mathfrak{C}$, *falls* $\mathfrak{C} = \mathsf{Mod}(\Delta)$
2. ***axiomatisiert*** *einer* ***Theorie*** Γ, *falls* $\mathsf{Th}(\mathsf{Mod}(\Delta)) = \Gamma$.

Man nennt Δ *dann die Axiome von* Γ *bzw.* $\mathfrak{C}$.

Es ist normalerweise unser Wunsch, Klassen und Theorie mit möglichst wenigen (und kurzen) Axiomen zu charakterisieren. Jetzt aber erstmal ab ins "Konkrete".

17.1 Partielle Ordnungen

Partielle Ordnungen sind Strukturen mit einer Relation die man normalerweise $\leq$ schreibt. Um Syntax und Semantik auseinanderzuhalten, nutzen wir $\leq$ als Prädikate der logischen Sprache, $\preceq \subseteq U^2$ als dessen Interpretation. Die Axiome sind folgende:

(trans)	$\forall xyz.[(x \leq y \wedge y \leq z) \rightarrow x \leq z]$
(refl)	$\forall x.x \leq x$
(anti)	$\forall xy.[(x \leq y \wedge y \leq x) \rightarrow x = y]$

Partielle Ordnungen sind sehr wichtig in vielen Anwendungen. Intuititiv beschreiben sie Strukturen, deren Objekte teilweise untereinander geordnet sind, teilweise aber auch nicht vergleichbar. Einige Beispiele:

- Partielle Ordnungen bekommt man, wenn man Objekte vergleicht, die verschiedene Merkmale haben: z.B. Autos in Bezug auf Merkmale PS, Hubraum, Gewicht, Reichweite etc.: die einzelnen Merkmale sind lineare Ordnungen, aber zwei Autos können oft nicht geordnet werden nach der *Gesamtheit der Merkmale*.

- Ein weiteres Beispiel ist Informativität: eine Aussage kann informativer sein als eine andere, aber oftmals sind sie *unvergleichbar*, einfach weil sie ganz verschiedene Informationen geben.

- Partielle Ordnungen sind auch das Rückgrat von Ontologien. Intuitiv ist das eine Beschreibung der Welt nach Kategorien:

  - Stuhl$\subset$Artefakt, Stuhl$\subset$Sitzgelegenheit,
  - aber Artefakt$\not\subset$Sitzgelegenheit, Artefakt$\not\supset$Sitzgelegenheit

  Kategorien sind also partiell geordnet.

- Und damit kommen wir auch schon zu der wohl bekanntesten partiellen Ordnung: die mengentheoretische Relation $\subseteq$ (also Teilmenge). Das ist, auf einer beliebigen Menge von Mengen, immer einer partielle Ordnung.

Aufgabe

Zeigen Sie, dass die Relation $\leq$ wie wir sie für Boolesche Algebren definiert haben, für jede Boolesche Algebra eine partielle Ordnung ist.

17.2 Lineare Ordnungen

Ein Spezialfall von partiellen Ordnungen sind lineare Ordnungen, in denen die Individuen wie auf einer Kette aufgereiht sind. Dafür gibt es viele Beispiele, z.B. die Strukturen $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ (die rationalen Zahlen), $(\mathbb{R}, \leq)$ (die reellen Zahlen). Das Axiom, mit dem partielle Ordnungen zu linearen Ordnungen werden, ist folgendes:

(lin) $\forall xy.(x \leq y \vee y \leq x)$

Das bedeutet: alle Objekte sind vergleichbar. Die Strukturen mir $\mathbb{N}$ und $\mathbb{Z}$ unterscheiden sich dadurch, dass die erste ein minimales Elemente hat (1 bzw. 0).

Aufgabe

Geben Sie das Axiom, das sicherstellt eine Struktur hat ein minimales Element.

Lösung: $\exists x.\forall y.x \leq y$

$\mathbb{N}$ und $\mathbb{Z}$ unterscheiden sich von $\mathbb{Q}$ und $\mathbb{R}$ dadurch, dass sie **diskret** sind: in $\mathbb{Q}$ können wir zwei beliebige Individuen nehmen, wir werden immer ein drittes finden, das zwischen ihnen liegt (In Bezug auf $\leq$).

Aufgabe

Geben Sie das Axiom, das sicherstellt dass die Ordnung diskret ist.

Lösung (eine von vielen): wir definieren zunächst das Gegenteil, nämlich **Stetigkeit**. Das geht wie folgt:

$$\forall xy.\exists z.[x \leq y \wedge \neg(x = y) \rightarrow (x \leq z \wedge z \leq y \wedge \neg(x = z) \wedge \neg(z = y)]$$

Das besagt, dass zwischen zwei beliebigen Elementen ein drittes liegt. Diskretheit ist nicht einfach die Negation; wir müssen schauen dass jedes Element einen unmittelbaren Nachfolger hat. Um diese Aufgabe zu lösen, ist es recht praktisch, eine Relation $<$ zu haben, die sich wie $\leq$ verhält, aber **intransitiv** ist, also $x \not< x$ erfüllt. Die gibt es nicht in unserer Sprache, aber:

wir können sie in unserer Sprache **definieren**, so wie wir in Aussagenlogik neue Konnektoren definiert haben. Die Definition lautet:

(30) $x < y \equiv x \leq y \wedge \neg(x = y)$

Wir definieren also ein neues Symbol y auf der linken Seite von $\equiv$; auf der rechten Seite steht eine **offene** Formel, deren freie Variablen die Stelligkeit der neuen Relation bestimmen. Damit gibt es folgende einfache und elegante Definition:

(diskr) $\forall x.\exists z.\forall y.x < y \rightarrow (x < z \wedge z \leq y)$

Aufgabe

Geben Sie das Axiom, das sicherstellt dass die Ordnung stetig ist, d.h. zwischen zwei Elementen *immer* ein drittes liegt. Lösung:

(kont) $\forall xy\exists z.(x < y) \rightarrow (x < z \wedge z < y)$

Übung 10

Nehmen Sie die Axiome der partiellen Ordnungen, sowie folgende Axiome:

(8a) $\exists x.\forall y.x \leq y \vee y \leq x$
(8b) $\forall xyz.(\neg x \leq y \wedge \neg y \leq x) \rightarrow (x \leq z \vee z \leq x \vee y \leq z \vee z \leq y)$
(8c) $\forall xyz.(x \leq y \wedge y \leq z) \rightarrow (x = y \vee y = z)$
(8d) $\forall xyz.(x < z \wedge \neg y \leq z) \rightarrow x \leq y$

($<$ wie oben definiert) Was besagen diese beiden Axiome einzeln für sich in der Theorie der partiellen Ordnungen? Was bedeuten sie für ihre Modelle, wie kann man alle Modelle graphisch anschaulich darstellen?

Aufgabe

Definieren Sie (innerhalb der Theorie der diskreten linearen Ordnungen) eine Relation $UN(x, y)$, die soviel besagen soll wie: y ist der unmittelbare Nachfolger von x.

Lösung: $UN(x, y) := x < y \wedge (\neg\exists z.(x < z \wedge z < y))$

Wenn wir neue Prädikate definieren, können wir sie als auflösbare Abkürzungen jederzeit und frei benutzen; das macht uns das Leben in vieler Hinsicht einfacher.

Jetzt kann ich Sachen schreiben wie:

(31) $\forall x.\exists y.\, UN(x, y)$

Wichtig: Die Stelligkeit eines definierten Prädikates ist bestimmt durch die freien Variablen der Formel, die es definiert!

Aufgabe

Definieren Sie (innerhalb der Theorie der linearen/partiellen Ordnungen) $min(x)$, d.h. x ist minimal. Vorsicht: im partiellen Fall ist die Frage: eindeutig minimal (kleines als alles) oder uneindeutig minimal (nichts ist kleiner)

Frage: Wir haben an einer Stelle gesagt, kontinuierlich heißt: zwischen zwei beliebigen ungleichen Punkten liegt ein dritter, an anderer: zwischen zwei beliebigen ungleichen Punkten liegen unendlich viele. Besteht ein Unterschied zwischen den beiden Aussagen? Und wenn ja welcher?

Antwort: Nein, denn wenn es zwischen Punkt 1 und 2 einen dritten gibt (nennen wir ihn 3), dann gibt es auch zwischen 1 und 3 einen vierten (nennen wir vier), zwischen 1 und 4 einen fünften usw. Alle diese (unendlich vielen) Punkte liegen aber zwischen 1 und 2!

Frage: Welches Axiom unterscheidet $(\mathbb{Q}, \leq)$ und $(\mathbb{R}, \leq)$?

Die Antwort lautet: gar keines! Man sagt dann auch: die Strukturen sind **elementar äquivalent**, was soviel bedeutet wie: sie sind durchaus

verschieden, aber mittels Prädikatenlogik können wir sie nicht auseinanderhalten! Formal:

$$\mathcal{M}, \mathcal{M}' \text{ sind elementar äquivalent} \overset{def}{\Longleftrightarrow} \mathcal{M} \in \mathsf{Mod}(\Delta) \Leftrightarrow \mathcal{M}' \in \mathsf{Mod}(\Delta)$$

Wir können also vieles sagen mittels Prädikatenlogik, aber bei weitem nicht alles. Das ist aber nicht unbedingt ein Nachteil! Z.B. können wir **isomorphe** Strukturen niemals unterscheiden.

Hotel Hilbert und Kantors Diagonale: Ein (Weihnachts)märchen
Aber was genau unterscheidet $\mathbb{Q}$ und $\mathbb{R}$, woher wissen wir dass die beiden nicht isomorph sind? Die Antwort lautet: $\mathbb{R}$ ist vie größer als $\mathbb{Q}$!

17.3 Endlichkeit und Wohlordnung (Exkurs)

Wir sagen, eine lineare Ordnung $(M, \preceq)$ ist **wohlgeordnet**, falls gilt: für alle $x \in M$ ist die Menge

$$\{y : y \preceq x\}$$

endlich; der Logiker schreibt auch:

$$\{y : y \preceq x\}| < \omega \ (\omega = |\mathbb{N}|)$$

ist die Kardinalität der natürlichen Zahlen). Z.B. sind die natürlichen Zahlen wohlgeordnet, die ganzen Zahlen nicht (jede Wohlordnung hat ein minimales Element!); außerdem muss jede Wohlordnung diskret sein. Andersrum ist natürlich jede endliche lineare Ordnung eine Wohlordnung.

Jetzt gibt es allerdings ein Problem: in Prädikatenlogik kann man so etwas wie "eine Menge ist endlich" nicht ausdrücken; wir können ja nur über Individuen reden, nicht über Mengen. Also haben wir hier auch eine intrinsische Beschränkung unserer Sprache.

Aufgabe: Definieren Sie eine lineare Ordnung $(M, \preceq)$ (als Modell, also nicht logisch), in der gilt: 1. M ist diskret, 2. M hat ein maximales und minimales Element, und 3. M ist unendlich.

17.4 Bäume

Bäume haben Sie hoffentliche bereits kennengelernt, als geordnete Strukturen, die auseinander verzweigen, aber in denen Zweige niemals zusammenkommen, und die außerdem eine Wurzel haben. Wir nehmen erstmal Bäume an, die nur die sog. **Dominanzrelation** haben, also unvergleichbare Knoten untereinander nicht geordnet sind. In diesem Fall sind Bäume ein speziallfall von partiellen Ordnungen, wir nehmen also diese Axiome und gesellen folgende hinzu:

(wurz) $\exists x.\forall y.x \leq y$
(vlin) $\forall xyz.[(x \leq z \wedge y \leq z) \rightarrow (x \leq y \vee y \leq x)]$

Das reicht auch schon: (wurz) sagt wir haben ein minimales Element (die Wurzel), (vlin) sagt dass für jeden Knoten die Menge seiner Vorgänger linear geordnet ist - das bedeutet: von Blatt zu Wurzel gesehen verzeigt die Struktur niemals, also andersrum, zwei Zweige wachsen nie zusammen.

Die Bäume, die sie wahrscheinlich kennen, sind noch etwas anders, sie haben nicht nur eine Dominanzrelation, sondern auch eine Präzedenzrelation. Die erfüllt natürlich gewisse Eigenschaften, die sich sehr gut anhand von gezeichneten Bäumen ablesen lassen;z.B. sollen sich Kanten nicht kreuzen dürfen.

Übung 11

Nehmen sie geordnete Bäume als Strukturen $(M, \preceq, \sqsubset)$, wobei $\preceq$ die Dominanzrelation ist (axiomatisiert durch die obigen Axiome), und $\sqsubset$ die (irreflexive) Präzedenzrelation. Diese Relation soll, wenn Sie Bäume aufzeichnen, dafür stehen dass gewisse Knoten links/rechts von anderen stehen. Beachten Sie:

- Die Relation $\sqsubset$ "vererbt sich" sich über $\preceq$, d.h. es gibt keine kreuzenden Kanten.
- Zwei Knoten stehen in der Relation $\preceq$ zueinander, genau dann wenn Sie *nicht* in der Relation $\sqsubset$ zueinander stehen.

Liefern Sie die Axiome für die Klasse der geordneten Bäume, also die Axiome, deren endliche Modelle Bäume sind, die Sie in der Ebene aufzeichnen können.

Die Axiome für $\preceq$ haben wir bereits; wir brauchen noch die für $\sqsubset$ und die Interaktion der beiden!

Lösung

Geordnete Bäume haben eine weitere Ordnung über den Knoten. Derartige Bäume entsprechen den Graphen, die wir üblicherweise zeichnen. Wir denotieren diese Ordnung mit $\sqsubset$. Wir brauchen zunächst die Axiome, die eine **strenge partielle Ordnung** garantieren, das ist eine irreflexive PO:

(Ax15) $\forall x.\neg x \sqsubset x$ (Irreflexivität)

(Ax16) $\forall xy.(x \sqsubset y \rightarrow \neg y \sqsubset x)$ (Asymmetrie)

(Ax17) $\forall xyz.(x \sqsubset y \wedge y \sqsubset z) \rightarrow x \sqsubset z$ (Transitiviät)

Man beachte dass zusätzlich Antisymmetrie ersetzt durch Asymmetrie: gegeben Irreflexivität sind die beiden äquivalent, aber Asymmetrie ist wohl einfacher und klarer.

Als nächstes kommt die entscheidenden Axiome, die garantieren dass $\sqsubset$ und $\leq$ auf die gewünschte Art und Weise interagieren. Was wir wollen ist:

> Zwei verschiedene Knoten sind in der $\sqsubset$-Relation, genau dann wenn sie nicht in der $\leq$-Relation zueinander stehen.

Das geht wie folgt:

(Ax18) $\forall xy.[(\neg((x \sqsubset y \vee y \sqsubset x) \wedge (x \leq y \vee y \leq x)) \wedge ((x \sqsubset y \vee y \sqsubset x) \vee (x \leq y \vee y \leq x))]$ (Vollständigkeit)

Das ist die sehr explizite Variante, ohne Abkürzungen. Die Kurzform ist:

(Ax18') $\forall xy.(\neg(x \leq y \vee y \leq x)) \leftrightarrow (x \sqsubset y \vee y \sqsubset x))$

Was wir weiterhin wollen ist dass sich die Ordnung $\sqsubseteq$ über die Relation $\leq$ "vererbt"; graphisch gesprochen, wir möchten, dass wir unseren Baum *ohne*

kreuzende Kanten zeichnen können. Das geht wie folgt:

(Ax19) $\forall xy.x \sqsubset y \rightarrow [\forall uz.(x \leq u \wedge y \leq z) \rightarrow u \sqsubset z]$

Sprich: $\sqsubset$ vererbt sich von (x, y) auf (u, z), vorausgesetzt dass $x \leq u$, $y \leq z$. So bekommen wir die **Axiome der Theorie der geordneten Bäume**:

(trans)	$\forall xyz.[(x \leq y \wedge y \leq z) \rightarrow x \leq z]$
(refl)	$\forall x.x \leq x$
(anti)	$\forall xy.[(x \leq y \wedge y \leq x) \rightarrow x = y]$
(wurz)	$\exists x.\forall y.x \leq y$
(vlin)	$\forall xyz.[(x \leq z \wedge y \leq z) \rightarrow (x \leq y \vee y \leq x)]$
(Ax15)	$\forall x.\neg x \sqsubset x$ (Irreflexivität)
(Ax16)	$\forall xy.(x \sqsubset y \rightarrow \neg y \sqsubset x)$ (Asymmetrie)
(Ax17)	$\forall xyz.(x \sqsubset y \wedge y \sqsubset z) \rightarrow x \sqsubset z$ (Transitiviät)
(Ax18')	$\forall xy.(\neg(x \leq y \vee y \leq x)) \leftrightarrow (x \sqsubset y \vee y \sqsubset x))$
(Ax19)	$\forall xy.x \sqsubset y \rightarrow [\forall uz.(x \leq u \wedge y \leq z) \rightarrow u \sqsubset z]$

17.5 Hausaufgabe zum 17.1.2022

Schreiben Sie ein Axiom für folgende Eigenschaft von Bäumen:

- Bäume sollen binär sein, d.h. sie haben entweder 2 unmittelbare Nachfolger oder keinen.

Hier brauchen Sie evtl. das Prädikat $UN(x, y)$!

18 Definierbarkeit von Prädikaten und die Bedeutung von offenen Formeln in Theorien

Axiome axiomatieren eine Klasse von Modellen, in unserem Fall die geordneten Bäume. Axiome sind *immer geschlossene Formeln*, denn nur geschlossene Formeln sind wahr/falsch in Modellen. Axiome axiomatisieren auch eine **Theorie**, d.i. die Menge der Formeln, die daraus folgen.

Gegeben eine Theorie, können wir nun neue Prädikate **definieren**. Zur Klärung des Begriffs:

- Die Definition eines Prädikates $P_{neu}(x_1, ..., x_n)$ (in einem festgelegten Vokabular, und im Rahmen einer Theorie) ist immer eine **offene Formel** $\alpha(x_1, ..., x_n)$ in unsere, Vokabular

- Man schreibt dann

  (32) $P_{neu}(x_1, ..., x_i) := \alpha(x_1, ..., x_i)$

  Die Variablen $x_1, ..., x_n$ des definierten Prädikates sind genau die freien Variablen der Formel $\alpha(x_1, ..., x_i)$ – nicht mehr und nicht weniger!

- Eine Definition in diesem Sinne ist eine *syntaktische Abkürzung*. Wenn wir irgendwo, auch im Rahmen einer größeren Formel, $P_{neu}(x_1, ..., x_n)$ schreiben, dann tun wir das nur als Abkürzung für $\alpha(x_1, ..., x_i)$!

Wir fügen unserem Vokabular also ein neues Wort hinzu, allerdings eines das wir nicht brauchen – wir können nicht mehr sagen, aber wir können die Dinge damit kürzer sagen. Etwa so, wie wenn ich definiere:

(33) glau := grau oder blau

Soweit die syntaktische Perspektive. Semantisch gesprochen definiert eine offene Formel eine **Relation**, in jedem Modell: sei $M = (U, ...)$ ein Modell; dann ist die Bedeutung von $\alpha(x_1, ..., x_i)$ in M die Menge

$$\{(a_1, ..., a_i) \in U^n : M, \sigma \models \alpha(x_1, ..., x_i)\},$$

wobei $\sigma(x_1) = a_1$,..., $\sigma(x_n) = a_n$. Wir legen also fest, wie die Variablen der Formeln interpretiert werden. Z.B. mit der obigen Definition, innerhalb der Theorie der partiellen Ordnung,

(34) $x < y := x \leq y \wedge \neg x = y$

definieren wir die strenge Ordnung (irreflexiv). Das gilt hier für alle partiellen Ordnungen! In diesem Sinne können wir übrigens auch das Gegenteil machen: gegeben eine strenge Ordnung wie $\sqsubset$, können wir definieren:

(35) $x \sqsubseteq y := x \sqsubset y \vee x = y$

Das wäre dann die reflexive Variante dazu! Man sagt dann übrigens: die Ordnungen $<$ und $\leq$ sind **interdefinierbar**. Viele weitere Beispiele in der folgenden Übung.

Übung

Wir sind in der Theorie der (ungeordneten) Bäume.

1. Definieren Sie die Relation des unmittelbaren Nachfolgers bzg. $\leq$ (Dominanz)

2. Definieren Sie die Relation: Geschwister $g(x, y)$, die für alle Knoten mit denselben Vorgängern gilt. Hier bedeutet also unmittelbare Dominanz soviel wie: Elternschaft.

3. Definieren Sie dementsprechend das Prädikat: Cousins $c(x, y)$

4. Definieren Sie die Prädikate $wurzel(x)$ (minimal für $\leq$), $blatt(x)$ (maximal für $\leq$)

Übung

1. Axiomatisieren Sie Bäume *ohne Blätter* (also unendlich in alle Richtungen!)

   Lösung: $\neg\exists x.blatt(x)$, oder äquivalent: $\forall x.\neg blatt(x)$

2. Axiomatisieren Sie binäre Bäume (entweder 2 oder kein Nachfolger)

   Lösung: $\forall x.blatt(x) \vee [\exists yz.((elter(x, y) \wedge elter(x, z) \wedge \neg y = z)$ $\wedge\forall u.elter(x, u) \rightarrow (u = y \vee u = z)]$

3. Axiomatisieren Sie Bäume, die den Ableitungen von regulären Grammatiken entsprechen!

   Lösung: (nicht ganz vollständig: hat den trivialen Baum mit einem Knoten als Modell, und hat ebenfalls unendliche Modelle)

   $\forall x.[\neg blatt(x) \rightarrow [\exists yz.(elter(x, y) \wedge elter(x, z) \wedge blatt(y) \wedge \neg blatt(z) \wedge y \sqsubset z)]]$

Hausaufgabe zum 24.1.22

Axiomatisieren Sie Bäume, die den Ableitungen von regulären Grammatiken entsprechen, aber diesmal in der Theorie der vollständig geordnete Bäume. Beachten Sie insbesondere die Ordnung von Terminal/Nichtterminal!

Übung 10

Wir können uns vorstellen, es gibt einen Quantor $\exists x!\alpha$, mit der Bedeutung "es gibt genau ein x dass α erfüllt" (technischer: genau eine Belegung in der Äquivalenzklasse). Definieren Sie diesen Quantor mit unseren bekannten Quantoren und Konnektoren. NB: α ist eine Variable (für eine beliebige Formel) in dieser Definition!

Diese Aufgabe zeigt uns, dass wir uns also auch verschiedende Quantoren definieren können.

Lösung:

$$\exists x.[\alpha \wedge \forall y.(\alpha[y/x] \rightarrow x = y]$$

18.1 Analysis und Körper

Eine andere Struktur die wir sehr gut kennen sind die reellen Zahlen mit denselben Operatoren wie vorher, sowie zusätzlich mit den **inversen Operatoren** $-$ und :. Es ist sehr hilfreich, sich diese Axiome anzuschauen, da fast alle interessanten Axiome der allgemeinen Algebra darin vorkommen. Die Sprache ist ähnliche der Arithmetik, nur gibt es keine Nachfolger-Funktion. Die Axiome sind wie folgt:

$\forall xy.x \cdot y = y \cdot x$

$\forall xyz.x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(d.h. $(K, \cdot)$ ist eine Halbgruppe)

$\forall x.x \cdot 1 = x$

(d.h. $(K, \cdot, 1)$ ist ein Monoid)

$\forall x.\exists y.x \cdot y = 1$

(d.h. $(K, \cdot, [-]^{-1}, 1)$ ist eine Gruppe)

$\forall xy.x + y = y + x$

$\forall xyz.x + (y + z) = (x + y) + z$

($(K, +)$ ist eine Halbgruppe)

$\forall x.x + 0 = x$

(d.h. $(K, +, 0)$ ist ein Monoid)

$\forall x.\exists y.x + y = 0$

($(K, +, [-]^{-1}, 0)$ ist eine Gruppe)

$\forall xyz.x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

Das sind die Axiome eines Körpers. Es gibt tatsächlich nur sehr wenige unendliche Körper:

- $(\mathbb{Q}, +, \cdot, 0, 1)$
- $(\mathbb{R}, +, \cdot, 0, 1)$
- $(\mathbb{C}, +, \cdot, 0, 1)$ (die komplexen Zahlen)

Das Standardmodell dieser Formeln ist also die Analysis, wie wir sie kennen. Es gibt aber auch in diesem Fall Nicht-Standardmodelle. Ein besonders interessantes ist Analysis mit **infinitesimalen**, also unendlich kleinen (und großen) Quantitäten (man kennt das aus Ableitungen!).

19 Peano Arithmetik

Eine berühmte Theorie in der Geschichte der Logik ist die sog. **Peano Arithmetik**, die als logische Theorie unserer bekannten Arithmetik ($\mathbb{N}_0$ mit $+,\cdot$) dienen soll. Diese Theorie basiert auf der Annahme dass wir außer diesen beiden Funktionen noch eine dritte haben, nämlich die sog. Nachfolgerfunktion N, die für jede Zahl den unmittelbaren Nachfolger bezeichnet, also interpretiert wird als

(36) $N(x) = x + 1$

Unser Vokabular hat abgesehen von diesen entsprechenden Symbolen noch eine Konstante 0. Wir haben also folgendes Vokabular:

$$V_{PA} = (\Omega, +, \cdot, N, 0)$$

wobei $\Omega(+) = \Omega(\cdot) = 2$, $\Omega(N) = 1$, $\Omega(0) = 0$ (d.h. 0 ist eine Konstante). Wir möchten nun die Axiome finden, die sicherstellen, dass ein Modell sich wie unsere schulbekannte Arithmetik verhält, also die Struktur

$$(\mathbb{N}_0, +, \cdot, N, 0)$$

wobei $+, \cdot$ wie bekannt sind, und S wie in 36. Wir nennen diese Struktur $\mathbf{A}$. Die Axiome wurden zuerst von Giuseppe Peano aufgeschrieben, daher der Name.

$\forall x.\neg(N(x) = 0)$

$\forall xy.N(x) = N(y) \to x = y$

$\forall x.x + 0 = x$

$\forall xy.x + (N(y)) = N(x + y)$

$\forall xy.x \cdot N(y) = x + (x \cdot y)$

(optional)$\forall x \exists y.y = N(x)$

Die Theorie dieser Axiome nennen wir **PA**. Es ist leicht zu sehen dass $\mathbf{A} \models \mathbf{PA}$. Es ist auch möglich zu zeigen dass gilt:

1. $\mathbf{PA} \models \forall xy.x + y = y + x$
2. $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
3. $\mathbf{PA} \models \forall x.x \cdot 0 = 0$
4. $\mathbf{PA} \models \forall x.x \cdot 1 = x$

Beweis 1: Machen die Induktion über x, y. Sei $x, y = 0$. Dann ist $0+0 = 0$. Weiterhin: $x + N(y) = N(x + y) = N(y + x) = N(y) + x$. Ebenso: $N(x)+0 = N(x)$; $N(x)+N(y) = N(N(x+y)) = N(N(y+x)) = N(y)+N(x)$ etc.

Beweis 2: Induktion über x, y: $x = 0 = y$ ist klar. Nimm nun $N(x) + y$. Dann ist $N(x+y)\cdot z = z+((x+y)\cdot z) = z+(x\cdot z)+(y\cdot z) = (N(x)\cdot z)+(y\cdot z)$. Dasselbe andersrum.

Beweis 3: Wir haben $N(x) \cdot 0 = 0 + x \cdot 0 = x \cdot 0$. Also gilt: für alle x, y haben wir $x \cdot 0 = y \cdot 0$, also insbesondere, $x \cdot 0 = (x + x) \cdot 0$. Allerdings: $(x \cdot 0) + (x \cdot 0) = (x + x) \cdot 0 = x \cdot 0$. Also kann $x \cdot 0$ nicht der Nachfolger eines Objektes sein, also ist $x \cdot 0 = 0$, das einzige Objekt das kein Nachfolger ist.

Beweis 4: Geradeaus aus 3.

Was die Logiker interessierte waren vor allem folgende Fragen:

1. Gilt dass $\mathsf{Mod}(\mathbf{PA}) = \mathbf{A}$ (bis auf Isomorphie), also wird unsere bekannte Arithmetik eindeutig axiomatisiert?
2. Falls nein, gibt es eine endliche Erweiterung unserer Axiome, die das gewährleistet?
3. Können wir für jede Formel α entscheiden, ob $\mathbf{PA} \models \alpha$? Also ist die Theorie der Peano Arithmetik entscheidbar?
4. Können wir für jede Formel α entscheiden, ob $\mathbf{A} \models \alpha$, also können wir für jede Aussage über unsere Zahlen bestimmt sagen ob sie war oder falsch ist?

Alle diese Fragen waren von grundlegender Bedeutung für die frühe Logik (aus Gründen die etwas abführen). Heute wissen wir, die Antwort auf alle

diese Fragen lautet: **Nein**. Die Beweise hierfür sind komplex und faszinierend, und größtenteils Kurt Gödel geschuldet.

Eine entscheidbares Fragment der Peano Arithmetik ist die sog. **Presburger Arithmetik**, die das Fragment ohne $\cdot$ ist.

20 Definierbarkeit und die Bedeutung von offenen Formeln

Wie wir bereits gesehen haben, können wir innerhalb einer gegebenen Sprache und einer gegebenen Theorie gewisse Prädikate **definieren**. Eine Definition ist eine **offene Formel**, wobei die Anzahl der freien Variablen die Stelligkeit des Prädikates bestimmt. Ebenso wie definierte Konnektoren in der Aussagenlogik können wir definierte Prädikate frei benutzen, da sie nur Abkürzungen sind die wir jederzeit auflösen können. Sie bereichern also unsere Sprache (v.a. machen sie sie einfacher zu nutzen), ohne sie komplexer zu machen. Wir hatten die logische Definierbarkeit im Rahmen einer Theorie bereits nebenbei besprochen. Es gibt noch ein ganz interessantes Konzept, nämlich die **Definierbarkeit im Rahmen eines Modells**. Wir werden hier wie immer annehmen, dass wir ein gewisses Modell haben, und wann immer wir von logischen Formeln sprechen, meinen wir solche, die das passende Vokabular und eine passende Interpretation haben.

Wir nehmen nun folgende Konvention: nimm an, wir haben eine offene Formel α mit

$$FV(\alpha) = \{x_1, ..., x_i\}$$

Wir schreiben dann dafür $\alpha(x_1, ..., x_i)$; diese Schreibweise ist also eine Abkürzung um die freien Variablen zu indizieren. Sei nun

- $\mathcal{M}$ ein Modell mit Universum U,
- $\alpha(x_1, ..., x_i)$ eine offene Formel, und
- $a_1, ..., a_i \in U$.

Wir schreiben dann

$$\mathcal{M} \models \alpha(x_1, ..., x_i)[a_1, ..., a_i]$$

falls gilt:

$$\mathcal{M}, \sigma \models \alpha(x_1, ..., x_i)$$

falls $\sigma(x_1) = a_1$, ..., $\sigma(x_i) = a_i$. Wir können das machen, da es egal ist, was σ auf allen anderen Variablen macht – die kommen ja nicht frei vor. Nun können wir einen Schritt weitergehen: z.B. gegeben ein Modell $\mathcal{M}$ und eine

Formel $\alpha(x)$, können wir sagen dass $\alpha(x)$ in $\mathcal{M}$ eine Menge $X \subseteq U$, nämlich

(37) $\|\alpha\|^{\mathcal{M}} = \{a \in U : \mathcal{M} \models \alpha[a]\}$

Z.B. lassen wir $\mathcal{M}$ unsere Arithmetik **A** sein. Eine Frage, die man sich stellen kann ist:

Können wir in **P** die Menge der geraden Zahlen definieren?

Das ist nicht besonders schwer. Wir definieren erstmal die 2 als eine Abkürzung:

(38) $2 \equiv N(N(0))$

Nun schreiben wir:

(39) $\alpha_{ger}(y) \equiv \exists x.y = (2 \cdot x)$

Ebenso können wir beispielsweise die Primzahlen definieren:

(40) $\alpha_{prim}(x) \equiv \forall yz.[(x = y \cdot z) \rightarrow (x = y \vee z = y)]$

Bis jetzt haben wir Mengen definiert, was Formeln mit einer freien Variablen entspricht. Wenn wir dieses Konzept jetzt verallgemeinern, dann sehen wir dass Definierbarkeit Relationen (mit beliebiger Stelligkeit n) betrifft.

Wir können in der PA auch allgemeine mathematische Aussagen formulieren, wie etwa die berühmte starke Goldbachsche Vermutung:

Starke Goldbachsche Vermutung Jede gerade Zahl größer als 2 ist die Summe zweier Primzahlen.

Wir definieren zunächst einmal die Relation $<$:

(41) $x < y \equiv \exists z.x + z = y \wedge \neg z = 0$

Damit lässt sich die Vermutung wie folgt schreiben:

(42) $\forall x.\exists yz.[(\alpha_{ger}(x) \wedge 2 < x) \rightarrow (\alpha_{prim}(y) \wedge \alpha_{prim}(z) \wedge x = y + z)]$

Schwache Goldbachsche Vermutung Jede ungerade Zahl, die größer als 5 ist, ist Summe dreier Primzahlen. Diese Vermutung ist bewiesen unter der Annahme, dass die Riemannsche Vermutung richtig ist. ("Eine Zahl ist eine Primzahl gdw. wenn sie eine positive Nullstelle der Riemannschen ζ-Funktion ist").

Großer Fermatscher Satz/Fermats letzter Satz Sei $n > 2$. Dann hat die Gleichung $a^n + b^n = c^n$ keine Lösung mit $a, b, c \in \mathbb{N} - \{0\}$.

Der Satz wurde formuliert von Pierre de Fermat in 16??, aber bewiesen erst 1994.

Um das zu formulieren müssen wir Potenzen definieren; das geht, ist aber nicht gerade einfach.

Übung 10

Definieren Sie im Modell **A** folgende Mengen/Relationen:

1. Die Menge der Quadratzahlen.
2. Die Menge der Tripel $(n, m, o) \in \mathbb{N}^3$ für die gilt: n ist der größte gemeinsame Teiler von m, o.
3. Die Menge der Tripel $(n, m, o) \in \mathbb{N}^3$ für die gilt: $n \; mod \; m = o$ (die modulo Operation *mod* liefert den Rest bei ganzzahliger Division, z.B. $12 \; mod \; 5 = 2$.

Übung

1. Definieren Sie die Relation $pf(x, y)$, um zu sagen: x ist ein Primfaktor von y. (Also: Faktor und Primzahl).
2. Definieren Sie die Menge der Zweierpotenzen $\{2, 4, 8, 16, 32, ...\} = \{2^n : n \geq 1\}$. NB: Wir haben keine Potenzierung als Operation. Aber wenn Sie verstehen was das mit der vorigen Aufgabe zu tun hat, dann sind Sie schnell fertig.

Übung

Schwieriger: sei $\langle p_1, p_2, ..\rangle$ die (unendliche) Folge der Primzahlen. Der Beweis, dass es unendlich viele Primzahlen gibt, funktioniert mit Zahlen der Form

(43) $\Xi_n = (\Pi_{i=1}^{n} p_i) + 1$

Für diese Zahlen gilt: kein $p_i : i \leq n$ kann ein Primfaktor von ihr sein, also entweder

a Ξ_n ist selber eine Primzahl (man das Primordial, $3, 7, 31, 211$ etc.)

b Ξ_n hat einen Primfaktor grösser als p_n.

In jedem Fall kann p_n nicht die grösste Primzahl sein!

Definieren Sie die Menge der Zahlen der Form Ξ_n!

Übung

1. Definieren Sie die Relation $exp2(x, y)$, so dass gilt: $y = 2^x$
2. Eines der wichtigsten und fundamentalsten Ergebnisse der Arithmetik ist die **Eindeutigkeit der Primfaktorzerlegung**: jede Zahl lässt sich genau auf eine (bis auf Kommutation) Art und Weise als Produkt von Primzahlen darstellen. Wie schreiben wir das unserer Logik?

Das letztere Ergebnis liefert übrigens die Grundlage für die berühmte **Gödelisierung**: gegeben ein Alphabet lässt sich jedes Wort eindeutig als Zahl darstellen.

Lösung zu 1.: wir wären versucht folgendes zu schreiben:

(44) $(x = 0 \leftrightarrow y = 1) \wedge (\forall zu.(exp(x, y) \wedge x = N(z)) \leftrightarrow (y = 2 \cdot u \wedge exp(z, u))$

Das ist aber eine sogenannte **implizite Definition**: wir fügen das Prädikat $exp2$ zu unserer Sprache hinzu, und schreiben ein Axiom das seine Bedeutung regelt. Allerdings: $exp2$ gehört *nicht* zu unserer Sprache! Wir sollten also die implizite Definition in eine explizite Definition übersetzen: eine explizite Definition ist eine solche wie wir immer gemacht haben. Folgendes Theorem ist sehr wichtig:

Satz 17 *(Beths Definierbarkeitssatz) In Prädikatenlogik kann jede implizite Definition kann in eine explizite Definition überführt werden.*

Wie sieht also die explizite Definition von $exp2$ aus? Kompliziert! Insgesamt sieht das so aus

$mod(x, y, z) := \exists u.x = y \cdot u + z \wedge z < y$

$seq(x, y, z, u) := mod(a, (N(y \cdot N(z)), u)$

$seq(x, y, z, u)$ bedeutet soviel wie: u ist der $z$te Term in der Folge $xmody+1$, $x\ mod\ 2y + 1, x\ mod\ 3y + 1$

$exp2(y, z) :=$
$\exists zu.seq(z, u, 0, N(0)) \wedge seq(z, u, y, z) \wedge \forall vw.((v < y \wedge seq(z, u, v, w)) \rightarrow seq(z, u, N(v), 2 \cdot w))$

Etwas allgemeiner kann man definieren:

$pot(x, y, z) := \exists zu.seq(z, u, 0, N(0)) \wedge seq(z, u, y, z) \wedge \forall vw.((v < y \wedge seq(z, u, v, w)) \rightarrow seq(z, u, N(v), x \cdot w))$

wobei gilt: $\mathbf{A}, \sigma \models pow(x, y, z)$ gdw. $\sigma(z) = \sigma(x)^{\sigma}(y)$. Das ist allerdings nicht wirklich offensichtlich!

Aber auch wenn wir die explizite Definition nicht haben, wissen wir immer: wenn es eine implizite Definition gibt, dann gibt es eine explizite Definition

(45) $exp2(x, y) \equiv \phi(x, y)$

wobei $\phi(x, y)$ eine Formel in der Sprache der PA ist.

- das Prädikat $pf(x, y)$ haben wir definiert.
- ebenso die Menge $P2(x)$ der Zweierpotenzen
- $\leq$ ist klar

Hausaufgabe zum 31.1.2022

1. Definieren Sie das kleinste gemeinsame Vielfache zweier Zahlen, also $kgv(x, y, z)$.
2. Definieren Sie das Prädikat $sep(x, y)$, welches auf alle Zahlen m, n zutrifft für die gilt: das kleinste gem. Vielfache von m, n ist $m \cdot n$.

Lösung 1 Wieder am besten modular lösen:

$gv(x, y, z) := \exists uv.x \cdot u = z \wedge y \cdot v = z$

Das ist das gemeinsame Vielfache. Nun das kleinste:

$kgv(x, y, z) := gv(x, y, z) \wedge \forall z'.gv(x, y, z') \rightarrow z \leq z'$

Lösung 2 Ganz einfach:

$$sep(x, y) := \forall z.kgv(x, y, z) \to z = x \cdot y$$

Übrigens bedeutet das soviel wie: es gibt keine gemeinsamen Primfaktoren. Das ist nicht ganz offensichtlich, aber eigentlich klar: das gemeinsame Vielfache lässt sich ja sonst aus den "überlappenden Primfaktoren konstruieren.

21 Normalformen

21.1 Prenex Normalform

Es gibt viele Normalformen für Logik; wir werden hier eine spezielle betrachten, nämlich die sog. **Prenex Normalform** (PNF). Eine Formel in PNF hat die Form

$$Q.\alpha$$

wobei

- α eine **quantorenfreie** Formel ist, und
- Q eine Abfolge von Quantoren und Variablen ist.

Das heißt salopp gesagt: in PNF kommen erst alle Quantoren, und dann kommt der Rest. Ziel in diesem Abschnitt ist zu zeigen, dass es für jede Formel eine äquivalente Formel in PNF gibt. Zentral hierfür ist die Dualität

$$\exists x.\alpha \equiv \neg\forall x.\neg\alpha \tag{46}$$

$$\forall x.\alpha \equiv \neg\exists x.\neg\alpha \tag{47}$$

Wir zeigen wie wir mittels dieser Äquivalenzen Quantoren sukzessive nach außen bewegen können. Wir zeigen zunächst folgendes:

Lemma 18 *Nimm an, $x \notin FV(\alpha)$. Dann gilt:*

1. $\alpha \wedge \exists x.\beta \equiv \exists x.(\alpha \wedge \beta)$
2. $\alpha \vee \exists x.\beta \equiv \exists x.(\alpha \vee \beta)$
3. $\alpha \wedge \forall x.\beta \equiv \forall x.(\alpha \wedge \beta)$
4. $\alpha \vee \forall x.\beta \equiv \forall x.(\alpha \vee \beta)$

Das ist recht einfach zu sehen; wir zeigen 1. Für $\alpha \wedge \exists x.\beta$ brauchen wir $\sigma' \sim_x \sigma$, so dass

$$\mathcal{M}, \sigma \models \alpha \text{ und } \mathcal{M}, \sigma' \models \beta$$

Für $\exists x.(\alpha \wedge \beta)$ brauche wir

$$\mathcal{M}, \sigma' \models \alpha \text{ und } \mathcal{M}, \sigma' \models \beta$$

Da aber x in α nicht frei vorkommt, sind die Bedingungen äquivalent.

Dasselbe gilt natürlich für $(\exists x.\alpha) \wedge \beta$ etc.

Der $\rightarrow$ ist etwas schwieriger: wir haben $\alpha \rightarrow \beta \equiv \neg\alpha \vee \beta$, also folgt aus dem Lemma dass falls $x \notin FV(\alpha)$, dann $\alpha \rightarrow \exists x.\beta \equiv \exists x.(\alpha \rightarrow \beta)$. Allerdings gilt: falls $x \notin FV(\beta)$, dann

$$\begin{aligned}
(48) \qquad (\exists x.\alpha) \rightarrow \beta &\equiv (\neg\exists x.\alpha) \vee \beta \\
(49) \qquad &\equiv (\neg\neg\forall x.\neg\alpha) \vee \beta \\
(50) \qquad &\equiv (\forall x.\neg\alpha) \vee \beta \\
(51) \qquad &\equiv \forall x.(\neg\alpha \vee \beta) \\
(52) \qquad &\equiv \forall x.(\alpha \rightarrow \beta) \\
(53) \qquad &
\end{aligned}$$

Wir ändern also mit der negativen **Polarität** den Quantor. Das bringt uns folgendes Lemma:

Lemma 19 *Nimm an, $x \notin FV(\alpha)$. Dann gilt:*

1. $\alpha \rightarrow \exists x.\beta \equiv \exists x.(\alpha \rightarrow \beta)$
2. $\alpha \rightarrow \forall x.\beta \equiv \forall x.(\alpha \rightarrow \beta)$

Lemma 20 *Nimm an, $x \notin FV(\beta)$. Dann gilt:*

1. $(\exists x.\alpha) \rightarrow \beta \equiv \forall x.(\alpha \rightarrow \beta)$
2. $(\forall x.\alpha) \rightarrow \beta \equiv \exists x.(\alpha \rightarrow \beta)$
3. $\neg\exists x.\alpha \equiv \forall x.\neg\alpha$
4. $\neg\forall x.\alpha \equiv \exists x.\neg\alpha$

Hiermit können wir bereits den wichtigsten Satz beweisen:

Satz 21 *Für jede Formeln α gibt es eine Formel α' so dass*

1. $\alpha \equiv \alpha'$ *und*
2. α' *ist in PNF.*

Um das zu beweisen, können wir ganz einfach folgende Prozedur machen:

1. Alle gebundenen Variablen werden, zusammen mit dem Quantor, dergestalt umbenannt dass a) niemals zwei gleichnamige Variablen von verschiedenen Quantoren gebunden werden, und b) niemals zwei gleichnamige Variablen einmal gebunden und einmal frei auftreten. Das kann gemacht werden, ohne dass sich die Bedeutung der Formel ändert.

2. Dann wenden wir einfach schrittweise die vorhergenden Lemmas an, um nach und nach alle Quantoren nach außen zu verschieben. Da wir vorher Schritt 1 gemacht haben, ist sicher dass wir die Seitenbedingungen immer erfüllen.

Übung 11

Transformieren Sie folgende Formeln in PNF:

1. $\forall x.(P(x) \to \exists xy.Q(y,x))$

2. $\exists x.(\exists y.Q(x,y)) \to (\exists y.Q(y,x))$

3. $((\exists x.P_1(x)) \wedge (\exists y.P_2(y))) \to (\forall xy.Q(x,y))$

Lösung für 1
$\forall x.(P(x) \to \exists xy.Q(y,x))$
Schritt 1 (Variablen umbenennen):
$\forall x.(P(x) \to \exists zy.Q(y,z))$
Schritt 3 (Quantor heben):
$\forall x.\exists zy.(P(x) \to Q(y,z))$

Lösung für 2
$\exists x.(\exists y.Q(x,y) \to (\exists y.Q(y,x))$
Schritt 1 (Quantor heben):
$\exists x.\forall y.(Q(x,y) \to (\exists y.Q(y,x))$
Schritt 2 (Variablen umbenennen):
$\exists x.\forall y.(Q(x,y) \to (\exists z.Q(z,x))$
Schritt 3 (Quantor heben 2):
$\exists x.\forall y.\exists z.(Q(x,y) \to Q(z,x))$

Lösung für 3 (alternativer Lösungsweg):
$((\exists x.P_1(x)) \wedge (\exists y.P_2(y))) \rightarrow (\forall xy.Q(x,y))$
Schritt 1 (Variablen umbenennen):
$((\exists x.P_1(x)) \wedge (\exists y.P_2(y))) \rightarrow (\forall zu.Q(z,u))$
Schritt 2 (Quantoren heben 1):
$(\exists x.\exists y.(P_1(x)) \wedge P_2(y)) \rightarrow (\forall zu.Q(z,u))$
Schritt 3 (Quantoren heben 2):
$\forall x.\forall y.((P_1(x)) \wedge P_2(y)) \rightarrow (\forall zu.Q(z,u))$
Schritt 4 (Quantoren heben 3):
$\forall x.\forall y.\forall zu.((P_1(x)) \wedge P_2(y)) \rightarrow Q(z,u))$

Schritt 4 kann man wahlweise auch früher machen – die Reihenfolge der Allquantoren untereinander spielt ohnehin keine Rolle!

Übung 12

1. $(\neg\exists xy.P(x,y)) \rightarrow \neg\exists xy.Q(x,y)$
2. $(\exists x.\forall y.P(x,y)) \rightarrow (\forall y.\exists x.P(x,y))$

Hausaufgabe zum 20.1.20

Bringen sie folgende Formeln in PNF:

1. $((\exists x.\forall y.P(x,y)) \rightarrow (\exists z.Q(z))) \rightarrow (\forall xy.P(x,y))$
2. $\neg((\exists xy.P(x,y)) \rightarrow ((\exists x.Q(x)) \wedge (\exists y.R(y))))$

21.2 Die arithmetische Hierarchie

Sei α eine quantorenfreie Formel in der Sprache der Peano Arithmetik. Man sagt dann man:

- $\alpha \in \Sigma_0$, $\alpha \in \Pi_0$
- Nimm an, $\alpha \in \Sigma_n$, $\overline{x}$ eine Sequenz von Variablen. Dann ist $\forall \overline{x}.\alpha \in \Pi_{n+1}$
-
- Nimm an, $\alpha \in \Pi_n$, $\overline{x}$ eine Sequenz von Variablen. Dann ist $\forall \overline{x}.\alpha \in \Sigma_{n+1}$
- Wir definieren $\Delta_n = \Pi_n \cap \Sigma_n$

Man sagt, eine Formel ist Σ_n bzw. Π_n, wenn sie **logisch äquivalent** ist zu einer Formel in Σ_0 bzw. Π_n. Damit haben wir eine echte Hierachie:

$$\Pi_n \subsetneq \Pi_{n+1} \tag{54}$$

$$\Sigma_n \subsetneq \Pi_{n+1} \tag{55}$$

$$\Pi_n \subsetneq \Sigma_{n+1} \tag{56}$$

$$\Sigma_n \subsetneq \Sigma_{n+1} \tag{57}$$

Allgemein gilt: Δ_1 ist entscheidbar, Σ_1 rekursiv aufzählbar, alles jenseits davon ist unentscheidbar.

22 Entscheidbarkeit

22.1 Einleitung: Turing Maschinen

Achtung: dieser Abschnitt ist wesentlich unpräziser als die vorigen, oftmals werden technische Details einfach weggelassen. Hier geht es mir eher um das Konzeptuelle.

Das heute geläufigste Modell für universelle Berechenbarkeit ist die sog. Turingmaschine (TM). Das ist ein Automat

$$TM = (\Sigma, T, \Box, Q, q_0, q_f, A),$$

wobei

- Σ das Eingabealphabet ist;
- T das "interne" Rechenalphabet (Σ und T müssen nicht separat sein)
- $\Box$ ist das Leerzeichen, das eine wichtige Rolle spielt
- Q ist die Menge der Zustände der Maschine
- q_0 ist der Startzustand,
- q_f ist der akzeptierende Zustand
- $A \subseteq Q \times (\Sigma \cup T) \times (\Sigma \cup T) \times Q \times \{-1, 1\}$ sind die Arbeitsanweisungen der Maschine.

Die Maschine hat ein einseitig unendliches Band, auf dem zu Anfang das Eingabewort steht; außerdem hat sie einen Lese-Schreibkopf, der zu Anfang auf der Zelle ganz links steht. Eine Anweisung $(q, a, a', q', 1/-1)$ bedeutet:

- die Maschine ist in Zustand $q \in Q$,
- liest Buchstaben $a \in \Sigma \cup T$,
- schreibt dafür $a' \in \Sigma \cup T$,
- geht in Zustand $q' \in Q$.
- bewegt den Kopf nach links/rechts.

Die TM akzeptiert ein Wort w, wenn wir von dieser Eingabe auf dem ansonsten leeren Band in einen akzeptierenden Zustand kommen. Die TM weist ein Wort zurück, wenn sie von dieser Eingabe das leere Band erzeugt, aber nicht in q_f ist.

Auf diese Art und Weise können wir eine Sprache charakterisieren:

$$L(TM) = \{w \in \Sigma^* : TM \text{ akzeptiert } w\}$$

Man kann eine TM auch nutzen, um Funktionen zu berechnen: wir sagen:

$f_{TM}(w) = v$ gdw. TM mit Eingabe w in q_f kommt, und v steht auf dem Band.

Man kann natürlich auch eine Sprache als eine Funktion $f_{TM} : \Sigma^* \to \{0, 1\}$ auffassen. Die sog. **Church-Turing Hypothese** besagt: jede berechenbare Funktion kann von einer Turing Maschine berechnet werden. Anders gesagt: entweder eine Funktion kann von einer TM berechnet werden, oder sie kann gar nicht berechnet werden. Diese Hypothese kann natürlich nicht wirklich bewiesen werden, aber sie wurde bislang nicht falsifiziert.

22.2 Unentscheidbarkeit

Die Frage ist: können wir für jede beliebige TM, jede beliebiges w entscheiden ob $w \in L(TM)$? Alan Turing hat gezeigt, dass dieses Problem unentscheidbar ist, und damit die Mutter aller Unentscheidbarkeitsbeweise geschaffen.

Um diesen Beweis zu verstehen, braucht man zunächst folgendes: eine TM ist ein abstraktes mathematisches Modell; aber wir können dieses Modell auf einem Blatt Papier charakterisieren; ich kann z.B. eine TM einfach in diesem Skript aufschreiben. Das bedeutet, wir können Turingmaschinen als Wort kodieren. Dementsprechend gibt es die Abbildung

$$cod : \mathbf{TM} \to \Sigma^*$$

die Turingmaschinen als Worte beschreibt.

Als nächstes betrachten wir die **universelle Turingmaschine** UTM. Das ist eine Maschine, die das inverse von cod berechnet: wenn wir UTM die Eingabe $cod(TM)$ geben, dann berechnet es auf der nächsten Eingabe (abgetrennt mit sagen wir #) die Funktion f_TM, also

(58) $UTM(cod(TM)\#w) = f_{TM}(w)$

Diese Maschine ist universell, da sie jede TM-Funktion berechnen kann, mit der passenden Eingabe. UTM lässt sich tatsächlich konstruieren (das ist aber mühsam, wir lassen das aus).

Nun kann man die Menge der Turingmaschinen in zwei Klassen unterteilen:

1. $L_1 := \{TM : f_{TM}(cod(TM))) = 1\}$
2. $L_0 := \{TM : f_{TM}(cod(TM))) \neq 1\}$

Es gibt also Maschinen, die *ihre eigene Kodierung* akzeptieren, und solche, die sie zurückweisen. Nimm an, das Halteproblem oben ist entscheidbar. Dann ist jede TM entweder in L_1 oder L_0. Außerdem gibt es dann auch eine TM, die, gegeben $cod(TM)$ entscheiden kann, ob $cod(TM) \in L_1$ oder L_0 – sie muss ja nur als universelle Turingmaschine aus der Eingabe $cod(TM)$ die Eingabe $cod(TM)\#cod(TM)$ produzieren (einfach), und danach dass UTM Programm laufen lassen. Wir können nach unserer Annahme eine Maschine TM_{diag} (die Diagonalmaschine) konstruieren, so dass:

(59) $$f_{TM_{diag}}(cod(TM)) = \begin{cases} 1, \text{ falls } TM \in L_0 \\ 0, \text{ falls } TM \in L_1 \end{cases}$$

Nun stellt sich aber folgende Frage:

$$\text{Was ist } f_{TM_{diag}}(cod(TM_{diag}))?$$

Es gibt hier zwei Möglichkeiten:

1. $f_{TM_{diag}}(cod(TM_{diag})) = 1$. Dann ist $TM_{diag} \in L_0$, also per Definition $f_{TM_{diag}}(cod(TM_{diag})) = 0$ – Widerspruch!

2. $f_{TM_{diag}}(cod(TM_{diag})) = 0$. Dann ist $TM_{diag} \in L_1$, also per Definition $f_{TM_{diag}}(cod(TM_{diag})) = 1$ – Widerspruch!

Es gibt also in jedem Fall einen Widerspruch! Wie kann das sein? Nun, wir haben angenommen dass das Halteproblem entscheidbar ist, also wir für jede TM und jede Eingabe sagen können, ob die TM akzeptiert oder nicht. Das war offensichtlich eine falsche Annahme, denn sie führt auf einen Widerspruch! Das bedeutet: das Halteproblem ist unentscheidbar, und die Mengen L_1, L_0 sind nicht berechenbar: es gibt keine TM, die diese Mengen charakterisiert!

Definition 22 *Wir sagen eine Sprache $L \subseteq \Sigma^*$ ist **rekursiv aufzählbar**, falls es eine Turingmaschine TM gibt, so dass $L = \{w : f_{TM}(w) = 1\}$. Wir sagen eine Sprache $L \subseteq \Sigma^*$ ist **rekursiv**, falls L und $\Sigma^* - L$ rekursiv aufzählbar sind.*

Rekursiv bedeutet also soviel wie: entscheidbar. Rekursiv aufzählbar bedeutet soviel wie: semientscheidbar. Wir können also Worte irgendwie aufzählen, aber nicht für ein bestimmtes beantworten, ob es in der Menge ist.

Die Unentscheidbarkeit des Halteproblems zeigt sich anhand von vielen unentscheidbaren Problemen, die alle mehr oder weniger äquivalent sind. Die wichtigsten sind wie folgt:

1. Es gibt eine Sprache L für die es keine Turingmaschine TM gibt, so dass 1. $L(TM) = L$, und 2. TM auf jeder Eingabe hält.

2. Gegeben eine Turingmaschine TM und ein Wort w ist es im Allgemeinen nicht entscheidbar, ob $w \in L(TM)$.

3. Gegeben eine Turingmaschine TM und ein Wort w ist es im Allgemeinen nicht entscheidbar, ob TM mit Eingabe w jemals hält.

Diese Aussagen sind mehr oder weniger äquivalent. Sie haben noch eine weitere (schwächere) Konsequenz:

4. Gegeben eine Turingmaschine TM ist es im Allgemeinen unentscheidbar, ob $L(TM) = \emptyset$.

Das ist relativ klar: wenn wir nicht entscheiden können, ob ein bestimmtes Wort in $L(TM)$ ist, können wir um so weniger entscheiden ob *irgendein* Wort in $L(TM)$ ist (im Allgemeinen). Diese letzte Aussage ist besonders wichtig um die Unentscheidbarkeit der Prädikatenlogik zu beweisen.

22.3 Was hat das mit Prädikatenlogik zu tun?

Wir haben für Prädikatenlogik einen (vollständigen) Beweiskalkül; das zeigt schonmal folgendes:

Lemma 23 *Die Menge der Theoreme die Prädikatenlogik ist rekursiv aufzählbar.*

Das folgt aus unserem Beweiskalkül, den was der berechnen kann, kann eine Turingmaschine schon lange. Was wesentlich schwieriger zu zeigen ist, ist dass diese Menge nicht rekursiv ist:

Lemma 24 *Die Menge der Theoreme die Prädikatenlogik ist nicht rekursiv.*

Um dieses Lemma zu beweisen, muss man etwas ausholen. Betrachten wir zunächst folgende Fakten:

1. α ist ein Theorem gdw. $\neg\alpha$ ein Widerspruch ist gdw. $\neg\alpha$ kein Modell hat. Im Allgemeinen sind die Probleme also äquivalent.

2. Wir suchen nun eine Korresponenz $\alpha \approx TM$, so dass gilt: α hat kein Modell $\Longleftrightarrow L(TM) = \emptyset$.

3. Da die rechte Frage unentscheidbar ist, gilt das auch für die Frage, ob α ein Modell hat.

Allerdings können wir nicht das echte Halteproblem für Turingmaschinen in unserer Prädikatenlogik kodieren. Stattdessen brauchen wir ein etwas offeneres Konzept, nämlich die **Berechnungen** von Turingmaschinen. Das sind Folgen von Konfigurationen, die eine TM durchläuft. Konfigurationen können wir wie folgt beschreiben:

$$\langle wKv, q\rangle$$

wobei

- $wv \in (\Sigma \cup T)^*$ das (endliche) Wort auf dem Band ist (in der MAschine gefolgt von unendlich vielen Leerzeichen!)

- K bezeichnet den Kopf; wir schreiben den Kopf links der Position, in der er in der Maschine ist

- q ist der Zustand der Maschine

Konfigurationen bezeichnen Zustände, in denen Turingmaschinen sind wenn sie Berechnungen auf gewissen Eingaben vollführen. Dementsprechend können wir **Berechnungen** wie folgt definieren: eine Berechnung einer Turingmaschine TM ist eine endliche Folge

$$C_1 C_2 C_3 ... C_n$$

so dass C_1 etc. Konfigurationen von TM sind, und jeder Übergang von C_i nach C_{i+1} von den Anweisungen A von TM "gedeckt" ist (also legitim). Wir sagen nun: eine Berechnung

$$C_1 C_2 C_3 ... C_n$$

ist **akzeptierend**, falls gilt:

1. $C_1 = \langle Kw, q_0 \rangle$ für ein beliebiges $w \in \Sigma^*$
2. $C_n = \langle K, q_f \rangle$

Es ist klar das gilt:

$$L(TM) = \emptyset \qquad \Longleftrightarrow \qquad TM \text{ hat keine akzeptierende Berechnung}$$

Das bedeutet dass auch das rechte Problem unentscheidbar ist. Natürlich gilt:

- Berechnungen können kodiert werden als Worte.
- Worte können kodiert werden als endliche, linear geordnete Modelle

Wir können nun folgendes machen: wir nehmen eine Formel α_{TM}, so dass gilt:

- jedes Modell M von α_{TM} kodiert ein Wort (ist eine lineare Ordnung);
- und jedes kodierte Wort entspricht einer Berechnung.

Nun haben wir folgende Korrespondenz:

$$\alpha_{TM} \text{ hat ein Modell} \qquad \Longleftrightarrow \qquad TM \text{ hat eine akzeptierende Berechnung}$$

Da das rechte Problem unentscheidbar ist, ist auch das linke Problem unentscheidbar!

22.4 Entscheidbarkeit

Es gibt zwei Möglichkeiten, Prädikatenlogik entscheidbar zu machen:

- Wir beschränken unsere Benutzung der logischen Konnektoren oder Variablen; z.B. betrachten wir nur Formeln der Form $\exists \overline{x}.\alpha$, wobei α Quantorenfrei. Für derartige Fragemente kann man oft Entscheidbarkeit zeigen.
- Wir betrachten gewisse Theorien, z.B. die Theorie der linearen Ordnungen oder Bäume. Derartige Theorien sind oft entscheidbar, und dementsprechend sind auch *Erweiterungen* dieser Theorien (mit zusätzlichen Axiomen) entscheidbar.

Übung 12

Schreiben Sie eine Turingmaschine die folgende Sprachen erkennt/Funktionen berechnet:

1. $\{a^n b^n c^n : n \in \mathbb{N}\}$
2. $\{a^n : n \text{ eine Primzahl}\}$
3. $f_{TM}(n\#m) = n \cdot m$, wobei Zahlen jeweils repräsentiert werden als Binärziffern.

23 Fragmente

Entscheidbare Fragmente der Sprache gibt es viele. Nur kurz eine Übersicht:

- Beschränke die Anzahl der Variablen.
- Beschränke die Anzahl der problematischen Konnektoren, insbesondere $\neg, \rightarrow$
- Beschränke die Verwendung von Quantoren, z.B. nur einmalige Alternation oder keine Alternation.

Einige dieser Fragmente sind sehr wichtig in der Informatik und Computerlinguistik, z.B. Horn-Klauseln.

24 Entscheidbare Theorien

Gewisse Theorien sind entscheidbar, z.B. die Theorie der linearen Ordnugen, oder die Theorie der binären Bäume. Das ist sehr hilfreich für viele linguistische Anwendungen.

25 Zusammenfassung

Wir sind ausgegangen von der Fragestellung:

> Wir suchen eine Sprache, für die wir Wahrheit, Konsistenz, Widersprüchlichkeit und Konsequenz direkt an der syntaktischen Form ablesen können.

Haben wir unser Ziel erreicht?

- Teils ja: unsere Logiken haben vollständige, rein formale Beweistheorien, anhand derer wir Konsequenz ablesen können.
- Allerdings haben wir unser Problem der Unentscheidbarkeit: wir können die Fragen also **formalisieren**, aber **nicht mechanisieren**. Es bleibt also spannend!

Aber wir können trotzdem vieles daraus ziehen, wie z.B. das folgende:

Lemma 25 *Modell Existenz/Kompaktheit: Sei* Γ *eine Menge von Formeln, so dass jede endliche Teilmenge* $\Delta \subseteq \Gamma$ *konsistent ist, also* $\Delta \nvdash \bot$. *Dann existiert ein Modell von* Γ.

Das bedeutet: auch sehr seltsame Theorien haben Modelle (aber wir wissen nicht wie sie aussehen), vorausgesetzt ihre endlichen Teilmengen sind (beweistheoretisch) konsistent!