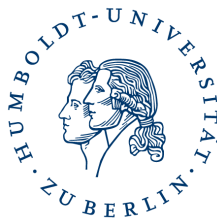


# Einführung in die formale Logik für IMP

Vorlesung im Sommersemester

Prof. Dr. Nicole Schweikardt

Lehrstuhl Logik in der Informatik  
Institut für Informatik  
Humboldt-Universität zu Berlin



Große Teile dieses Skripts basieren auf dem Skript zur Vorlesung „Logik in der Informatik“ von Prof. Dr. Nicole Schweikardt, HU Berlin



# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>5</b>
1.1	Von der Bibel bis zu den Simpsons . . . . .	5
1.2	Logik in der Informatik . . . . .	12
1.3	Lernziele, Semesterausblick und Literatur . . . . .	17
<b>2</b>	<b>Aussagenlogik</b>	<b>21</b>
2.1	Syntax und Semantik . . . . .	21
2.2	Aussagenlogische Modellierung . . . . .	47
2.3	Äquivalenz und Adäquatheit . . . . .	52
2.4	Normalformen . . . . .	64
2.5	Der Endlichkeitssatz . . . . .	73
2.6	Resolution . . . . .	78
2.7	Erfüllbarkeitsalgorithmen . . . . .	90
2.8	Hornformeln . . . . .	97
<b>3</b>	<b>Logik erster Stufe</b>	<b>105</b>
3.1	Strukturen . . . . .	105
3.2	Terme der Logik erster Stufe . . . . .	118
3.3	Syntax der Logik erster Stufe . . . . .	120
3.4	Semantik der Logik erster Stufe . . . . .	124
3.5	Beispiele für Formeln der Logik erster Stufe in verschiedenen Anwendungsbereichen . . . . .	141
3.6	Logik und Datenbanken . . . . .	144

3.7	Äquivalenz von Formeln der Logik erster Stufe . . . . .	151
3.8	Ehrenfeucht-Fraïssé-Spiele . . . . .	154
3.9	Erfüllbarkeit, Allgemeingültigkeit und die Folgerungsbeziehung	173
3.10	Normalformen . . . . .	175
<b>4</b>	<b>Grundlagen des automatischen Schließens</b>	<b>181</b>
4.1	Kalküle und Ableitungen . . . . .	182
4.2	Ein Beweiskalkül für die Logik erster Stufe — der Vollständig- keitssatz . . . . .	189
4.3	Der Endlichkeitssatz . . . . .	207
4.4	Die Grenzen der Berechenbarkeit . . . . .	214
4.5	Der Satz von Herbrand . . . . .	225
4.6	Automatische Theorembeweiser . . . . .	236
	<b>Literaturverzeichnis</b>	<b>239</b>

## *Kapitel 1*

# Einleitung

### 1.1 Von der Bibel bis zu den Simpsons

Folie 1

#### Logik

- altgriechisch „logos“: Vernunft
- die Lehre des vernünftigen Schlussfolgerns
- Teilgebiet u.a. der Disziplinen Philosophie, Mathematik, Informatik und Linguistik
- zentrale Frage:

*Wie kann man Aussagen miteinander verknüpfen, und auf welche Weise kann man formal Schlüsse ziehen und Beweise durchführen?*

Folie 2

#### Das Lügnerparadoxon von Epimenides

Brief des Paulus an Titus 1:12-13:

*Es hat einer von ihnen gesagt, ihr eigener Prophet:  
Die Kreter sind immer Lügner, böse Tiere und faule Bäume.*

### **Angenommen, die Aussage des Propheten ist wahr.**

Da der Prophet selbst Kreter ist, lügt er also immer (und ist ein böses Tier und ein fauler Bauch). Dann hat er aber insbesondere in dem Satz „*Die Kreter sind immer Lügner, böse Tiere und faule Bäume*“ gelogen. D.h. die Aussage des Propheten ist *nicht* wahr.

Dies ist ein Widerspruch!

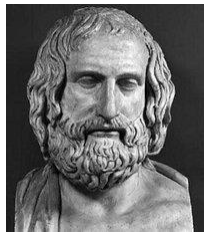
### **Angenommen, die Aussage des Propheten ist falsch.**

Dann gibt es Kreter, die nicht immer Lügner, böse Tiere und faule Bäume sind. Dies stellt keinen Widerspruch dar.

Insgesamt wissen wir also, dass der Prophet in seiner obigen Aussage nicht die Wahrheit gesagt hat.

Folie 3

## **Protagoras und sein Student Euthalus vor Gericht**



Protagoras (490 – 420 v.Chr.)

Quelle: <http://www.greatthoughtstresury.com/author/protagoras>

*Euthalus studierte die Kunst der Argumentation beim Meister Protagoras, um Anwalt zu werden.*

*Er vereinbart mit Protagoras, die Gebühren für den Unterricht zu bezahlen, sobald er seinen ersten Prozess gewonnen hat.*

*Aber dann zögert Euthalus seine Anwaltstätigkeit immer weiter hinaus, und schließlich beschließt Protagoras, seine Gebühren einzuklagen.*

*Euthalus verteidigt sich selbst ...*

Folie 4

### **Protagoras denkt:**

Wenn ich den Prozess gewinne, muss Euthalus gemäß Gerichtsbeschluss zahlen.

Wenn ich den Prozess verliere, muss Euthalus gemäß unserer Vereinbarung zahlen, da er dann seinen ersten Prozess gewonnen hat.

### **Euthalus denkt:**

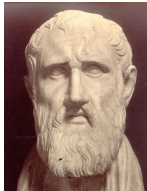
Wenn ich den Prozess gewinne, muss ich gemäß Gerichtsbeschluss nicht zahlen.

Wenn ich den Prozess verliere, muss ich gemäß unserer Vereinbarung nicht zahlen.

Folie 5

### **Achilles und die Schildkröte**

*Achilles und die Schildkröte laufen ein Wettrennen. Achilles gewährt der Schildkröte einen Vorsprung. Zenon behauptet, dass Achilles die Schildkröte niemals einholen kann.*



Zenon von Elea (490 – 425 v.Chr.) *Quelle:* <http://aefucr.blogspot.de/2008/04/resolucin-de-la-paradoja-de-zenn-de.html>

*Quelle:* <http://aefucr.blogspot.de/2008/04/resolucin-de-la-paradoja-de-zenn-de.html>

**Zenons Begründung:** Zu dem Zeitpunkt, an dem Achilles den Startpunkt der Schildkröte erreicht, ist die Schildkröte schon ein Stück weiter. Etwas später erreicht Achilles diesen Punkt, aber die Schildkröte ist schon etwas weiter. Wenn Achilles diesen Punkt erreicht, ist die Schildkröte wieder etwas weiter. So kann Achilles zwar immer näher an die Schildkröte herankommen, sie aber niemals einholen.

Folie 6

### **Auflösung durch die Infinitesimalrechnung:**



Gottfried Wilhelm von Leibniz (1646 – 1716)  
und Isaac Newton (1643 – 1727)

*Quelle:* <http://www-history.mcs.st-and.ac.uk/PictDisplay/Leibniz.html>  
und *Quelle:* [http://de.wikipedia.org/wiki/Isaac\\_Newton](http://de.wikipedia.org/wiki/Isaac_Newton)

**Bemerkung.** Aristoteles Auflösung dieses Paradoxons besteht darin, zu postulieren, dass man Strecken nicht unendlich Teilen kann. Aber auch ohne diese Annahme kann man das Paradoxon leicht mit Hilfe der Infinitesimalrechnung auflösen, denn die immer kürzer werdenden Strecken können insgesamt in beschränkter Zeit zurückgelegt werden. Leibniz und Newton waren die Begründer der Infinitesimalrechnung.

Folie 7

### Der Barbier von Sonnenthal

*Im Städtchen Sonnenthal (in dem bekanntlich viele seltsame Dinge passieren) wohnt ein Barbier, der genau diejenigen männlichen Einwohner von Sonnenthal rasiert, die sich nicht selbst rasieren.*

*Frage: Rasiert der Barbier sich selbst?*

#### **Angenommen, der Barbier rasiert sich selbst.**

Da er ein männlicher Einwohner von Sonnenthal ist, der sich selbst rasiert, wird er *nicht* vom Barbier rasiert. Aber er selbst ist der Barbier. Dies ist ein Widerspruch!

#### **Angenommen, der Barbier rasiert sich nicht selbst.**

Da er in Sonnenthal wohnt und dort alle Einwohner rasiert, die sich nicht selbst rasieren, muss er sich rasieren. Dies ist ein Widerspruch!

### *Die Anfänge der formalen Logik*

Folie 8

### **Aristoteles' Syllogismen**

Die folgende Schlussweise ist *aus rein formalen Gründen* korrekt.

*Annahme 1:* Alle Menschen sind sterblich.

*Annahme 2:* Sokrates ist ein Mensch.

*Folgerung:* Also ist Sokrates sterblich.

Diese Art von Schluss und eine Reihe verwandter Schlussweisen nennt man *Syllogismen*.



*Annahme 1:* Alle A sind B.  
*Annahme 2:* C ist ein A.  
*Folgerung:* Also ist C B.

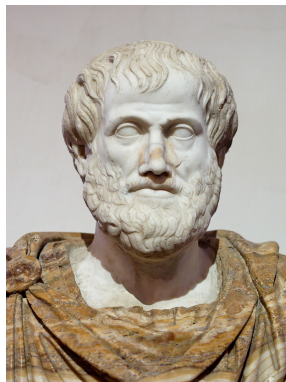
Folie 9

## Beispiele

*Annahme 1:* Alle Borg sind assimiliert worden.  
*Annahme 2:* Seven of Nine ist eine Borg.  
*Folgerung:* Also ist Seven of Nine assimiliert worden.

*Annahme 1:* Alle Substitutionschiffren sind  
anfällig gegen Brute-Force-Angriffe.  
*Annahme 2:* Die Julius-Cäsar-Chiffre ist eine Substitutionschiffre.  
*Folgerung:* Also ist die Julius-Cäsar-Chiffre anfällig  
gegen Brute-Force-Angriffe.

Folie 10



Aristoteles (384 - 322 v.Chr.)

Quelle: <http://de.wikipedia.org/wiki/Aristoteles>

Folie 11

## Ein komplizierterer formaler Schluss

<i>Annahme 1:</i> <u>Es gibt keine</u> Schweine, <u>die</u> fliegen können.
<i>Annahme 2:</i> <u>Alle</u> Schweine <u>sind</u> gefräßige Tiere.
<i>Annahme 3:</i> <u>Es gibt</u> Schweine.
<i>Folgerung:</i> <u>Also gibt es</u> gefräßige Tiere, <u>die nicht</u> fliegen können.

Die Form des Schlusses ist:

<i>Annahme 1:</i> <u>Es gibt keine</u> A, <u>die</u> B ( <u>sind</u> ).
<i>Annahme 2:</i> <u>Alle</u> A <u>sind</u> C.
<i>Annahme 3:</i> <u>Es gibt</u> A.
<i>Folgerung:</i> <u>Also gibt es</u> C, <u>die nicht</u> B ( <u>sind</u> ).

Folie 12



Charles Lutwidge Dodgson a.k.a. Lewis Carroll (1838 – 1898)

Quelle: [http://en.wikiquote.org/wiki/Lewis\\_Carroll](http://en.wikiquote.org/wiki/Lewis_Carroll)

*“Contrariwise,” continued Tweedledee, “if it was so, it might be;  
and if it were so, it would be; but as it isn’t, it ain’t.  
That’s logic.”*

aus: *Alice in Wonderland*

Folie 13

## Nicht jeder formale Schluss ist korrekt

<i>Annahme 1:</i> <u>Es gibt</u> Vögel, <u>die</u> fliegen können.
<i>Annahme 2:</i> <u>Es gibt keine</u> fliegenden (Tiere), <u>die</u> Klavier spielen können.
<i>Folgerung:</i> <u>Also gibt es keine</u> Vögel, <u>die</u> Klavier spielen können.

Kein korrekter Schluss, auch wenn in diesem Fall die Folgerung wahr ist.  
Der folgende, offensichtlich falsche, Schluss hat dieselbe Form:

<i>Annahme 1:</i> Es gibt Menschen, <u>die</u> stumm sind.
<i>Annahme 2:</i> <u>Es gibt keine</u> stummen (Lebewesen), <u>die</u> sprechen können.
<i>Folgerung:</i> <u>Also gibt es keine</u> Menschen, <u>die</u> sprechen können.

Folie 14

### Aber wie merkt man es?

Man kann einen falschen Schluss entlarven, indem man einen formal gleichen Schluss findet, der klar falsch ist.

<i>Annahme 1:</i> Erbeeren schmecken gut.
<i>Annahme 2:</i> Schlagsahne schmeckt gut.
<i>Folgerung:</i> Also schmecken Erdbeeren mit Schlagsahne gut.

Aber:

<i>Annahme 1:</i> Pizza schmeckt gut.
<i>Annahme 2:</i> Schlagsahne schmeckt gut.
<i>Folgerung:</i> Also schmeckt Pizza mit Schlagsahne gut.

Folie 15

### Wasons Auswahl Aufgabe (Wason's selection task)<sup>1</sup>

Uns stehen vier Karten der folgenden Art zur Verfügung:

Auf jeder Karte steht auf der Vorderseite eine Ziffer zwischen 0 und 9. Die Rückseite jeder Karte ist komplett rot oder komplett blau.

Wir sehen Folgendes:

---

<sup>1</sup>benannt nach Peter Cathcart Wason (1924–2003, Kognitiver Psychologe, London); in Wasons ursprünglicher Version der Auswahl Aufgabe handelt es sich um Karten, deren Vorderseiten Buchstaben und deren Rückseiten Ziffern enthalten, und die Hypothese ist „Wenn auf der Vorderseite der Karte ein Vokal steht, dann steht auf der Rückseite eine gerade Zahl“



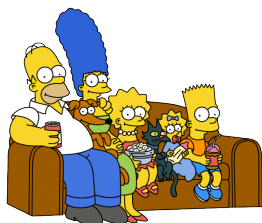
Jemand hat folgende **Hypothese** aufgestellt:

*Wenn auf der Vorderseite eine gerade Zahl steht,  
dann ist die Rückseite rot.*

Welche Karte(n) müssen Sie umdrehen, um zu überprüfen, ob die Hypothese stimmt?

Folie 16

**Und was sagen die Simpsons?**



Quelle: [http://en.wikipedia.org/wiki/Simpson\\_family](http://en.wikipedia.org/wiki/Simpson_family)

*Homer:* Not a bear in sight. The Bear Patrol must be working like a charm.

*Lisa:* That's specious reasoning, Dad.

*Homer:* Thank you, dear.

*Lisa:* By your logic I could claim that this rock keeps tigers away.

*Homer:* Oh, how does it work?

*Lisa:* It doesn't work.

*Homer:* Uh-huh.

*Lisa:* It's just a stupid rock.

*Homer:* Uh-huh.

*Lisa:* But I don't see any tigers around, do you?

*(Pause)*

*Homer:* Lisa, I want to buy your rock.

*[Lisa refuses at first, then takes the exchange]*

## 1.2 Logik in der Informatik

Folie 17

### Die Rolle der Logik in der Informatik

*Halpern, Harper, Immerman, Kolaitis, Vardi, Vianu (2001):*

*Concepts and methods of logic occupy a central place in computer science, inasmuch that logic has been called “the calculus of computer science”.*

aus: *On the unusual effectiveness of logic in computer science*, Bulletin of Symbolic Logic 7(2): 213-236 (2001)

Folie 18

## Anwendungsbereiche der Logik in der Informatik

- Repräsentation von Wissen (z.B. im Bereich der künstlichen Intelligenz) *[siehe Kapitel 2 und 3]*
- Grundlage für Datenbank-Anfragesprachen *[siehe Kapitel 3]*
- Bestandteil von Programmiersprachen (z.B. um Bedingungen in IF-Anweisungen zu formulieren) *[siehe Kapitel 2]*
- automatische Generierung von Beweisen (so genannte *Theorembeweiser*) *[siehe Kapitel 4]*
- Verifikation von
  - Schaltkreisen (*Ziel*: beweise, dass ein Schaltkreis bzw. Chip „richtig“ funktioniert)
  - Programmen (*Ziel*: beweise, dass ein Programm gewisse wünschenswerte Eigenschaften hat)
  - Protokollen (*Ziel*: beweise, dass die Kommunikation zwischen zwei „Agenten“, die nach einem gewissen Protokoll abläuft, „sicher“ ist — etwa gegen Abhören oder Manipulation durch dritte; Anwendungsbeispiel: Internet-Banking)
- Logik-Programmierung *[siehe folgende Folien]*

## *Kurze Einführung in die Logik-Programmierung*

Folie 19

### **„Was“ statt „Wie“ am Beispiel von Tiramisu**

#### **Tiramisu — Deklarativ**

Aus Eigelb, Mascarpone und in Likör und Kaffee getränkten Biskuits hergestellte cremige Süßspeise

(aus: DUDEN, Fremdwörterbuch, 6. Auflage)

#### **Tiramisu — Imperativ**

1/4 l Milch mit 2 EL Kakao und 2 EL Zucker aufkochen. 1/4 l starken Kaffee und 4 EL Amaretto dazugeben.

5 Eigelb mit 75 g Zucker weißschaumig rühren, dann 500 g Mascarpone dazumischen.

ca 200 g Löffelbiskuit.

Eine Lage Löffelbiskuit in eine Auflaufform legen, mit der Flüssigkeit tränken und mit der Creme überziehen. Dann wieder Löffelbiskuit darauflegen, mit der restlichen Flüssigkeit tränken und mit der restlichen Creme überziehen.

Über Nacht im Kühlschrank durchziehen lassen und vor dem Servieren mit Kakao bestäuben.

(aus: Gisela Schweikardt, handschriftliche Kochrezepte)

Folie 20

### **Der große Traum der Informatik**

#### **Imperative Vorgehensweise:**

Beschreibung, wie das gewünschte Ergebnis erzeugt wird ..... „Wie“

#### **Deklarative Vorgehensweise:**

Beschreibung der Eigenschaften des gewünschten Ergebnisses ..... „Was“

#### **Traum der Informatik:**

Möglichst wenig „wie“, möglichst viel „was“

D.h.: Automatische Generierung eines Ergebnisses aus seiner Spezifikation

#### **Realität:**

*Datenbanken:* Deklarative Anfragesprache ist Industriestandard (SQL)

*Software-Entwicklung:* Generierungs-Tools

*Programmiersprachen*: Logik-Programmierung, insbes. Prolog  
*ABER*: Imperativer Ansatz überwiegt in der Praxis

Folie 21

## Logik-Programmierung

- *Logik-Programmierung* bezeichnet die Idee, Logik direkt als Programmiersprache zu verwenden.
- *Logik-Programmierung* (in Sprachen wie *Prolog*) und die verwandte *funktionale Programmierung* (in Sprachen wie *LISP*, *ML*, *Haskell*) sind *deklarativ*, im Gegensatz zur *imperativen Programmierung* (in Sprachen wie *Java*, *C*, *Perl*).
- Die Idee der deklarativen Programmierung besteht darin, dem Computer lediglich sein *Wissen* über das Anwendungsszenario und sein *Ziel* mitzuteilen und dann die Lösung des Problems dem Computer zu überlassen.

Bei der imperativen Programmierung hingegen gibt man dem Computer die einzelnen Schritte zur Lösung des Problems vor.

Folie 22

## Prolog

- *Prolog*
  - ist die wichtigste logische Programmiersprache,
  - geht zurück auf Kowalski und Colmerauer (Anfang der 1970er Jahre, Marseilles),
  - steht für (franz.) *Programmation en logique*.
  - Mitte/Ende der 1970er Jahre: effiziente Prolog-Implementierung durch den von Warren (in Edinburgh) entwickelten Prolog-10 Compiler.
- Aus Effizienzgründen werden in Prolog die abstrakten Ideen der logischen Programmierung nicht in Reinform umgesetzt, Prolog hat auch „nichtlogische“ Elemente.

- Prolog ist eine voll entwickelte und mächtige Programmiersprache, die vor allem für *symbolische Berechnungsprobleme* geeignet ist.

Folie 23

## Anwendungen

Die wichtigsten Anwendungsgebiete sind die *künstliche Intelligenz* und die *Computerlinguistik*.

*Beispiele.* Das Interface für natürliche Sprache

- in der *International Space Station* wurde von der NASA
- beim IBM Watson System, das in 2011 die *Jeopardy! Man vs. Machine Challenge* gewonnen hat, wurde

in Prolog implementiert.

Mehr Informationen dazu finden sich z.B. unter

<https://sicstus.sics.se/customers.html> und

<http://www.cs.nmsu.edu/ALP/2011/03/>

[natural-language-processing-with-prolog-in-the-ibm-watson-system/](#)

Folie 24

## In der Veranstaltung *Einführung in die formale Logik für IMP*

... werden keine Details zur Programmiersprache Prolog oder dem allgemeinen Konzept der Logik-Programmierung behandelt.

Für alle, die sich diese Themen interessehalber im Selbststudium erarbeiten wollen, wird die folgende Literatur empfohlen:

- Kapitel 5 des Vorlesungsskripts [Sch18] und die im Übungsbetrieb der Veranstaltung *Logik in der Informatik* behandelten Übungsaufgaben zu den Themen *Prolog* und *Logik-Programmierung*,
- das Buch *Learn Prolog Now!* [BBS06], das einen guten Einstieg in die Programmiersprache Prolog bietet und
- das Buch *The Art of PROLOG* [SS94], das neben Details zur Programmiersprache Prolog auch eine Einführung in allgemeine Konzepte der Logik-Programmierung gibt.



## 1.3 Lernziele, Semesterausblick und Literatur

Folie 25

### Lern- und Qualifikationsziele

*Aus der Modulbeschreibung:*

Studierende erlangen die Fähigkeit, Sachverhalte in geeigneten formalen Systemen zu formalisieren und die grundlegenden Begriffe und Ergebnisse der mathematischen Logik zu verstehen und anzuwenden.

### Und was sagt Goethe dazu?

*Mein teurer Freund, ich rat Euch drum  
Zuerst Collegium Logicum.  
Da wird der Geist Euch wohl dressiert,  
In spanische Stiefeln eingeschnürt,  
Daß er bedächtiger so fortan  
Hinschleiche die Gedankenbahn,  
Und nicht etwa, die Kreuz und Quer,  
Irrlichteliere hin und her.*

Mephistopheles in *Faust*

Folie 26

### Semesterüberblick

1. Einleitung *(dieses Kapitel)*
2. Aussagenlogik  
*Syntax und Semantik, Normalformen, Modellierung,  
Resolution, Erfüllbarkeitsalgorithmen*
3. Logik erster Stufe  
*Syntax und Semantik, Normalformen, Modellierung,  
Nichtausdrückbarkeit*
4. Grundlagen des automatischen Schließens  
*Sequenzkalkül, Vollständigkeits- und Endlichkeitssatz,  
Grenzen der Berechenbarkeit, automatische Theorembeweiser*

Folie 27

## Literaturempfehlungen

Folgende Schriften werden zur Vertiefung des Vorlesungsstoffes empfohlen:

1. dieses Vorlesungsskript zur Veranstaltung *Einführung in die formale Logik für IMP*
2. das Lehrbuch [EFT07]
3. die Lehrbücher [Sch00, Bur98, KK06]

Als Ergänzung seien auch folgende Lehrbücher genannt:

- [Ebb03] (Einführung in die Mengenlehre)
- [Lib04, FG98] (Bücher zum Thema Logik und Komplexität)
- [Cam98, vD04, HR04] (weiterführende Literatur im Bereich Logik und automatisches Schließen)

*Auflösung zu Wasons Auswahl Aufgabe:*

Die Karte mit der „4“ und die blaue Karte müssen umgedreht werden.

Begründung:

- Falls die Rückseite der Karte mit der „4“ *nicht* rot ist, so haben wir ein Gegenbeispiel zur Hypothese gefunden und damit die Hypothese widerlegt.
- Falls die Vorderseite der blauen Karte eine gerade Zahl enthält, haben wir ein Gegenbeispiel zur Hypothese gefunden und damit die Hypothese widerlegt.
- Die Karte mit der „7“ brauchen wir nicht umzudrehen, da die Hypothese keine Aussage über die Rückseite von Karten mit ungeraden Ziffern macht.
- Die rote Karte brauchen wir nicht umzudrehen, da die Hypothese keine Aussage über die Vorderseite von Karten mit roter Rückseite macht.



## *Kapitel 2*

# Aussagenlogik

## 2.1 Syntax und Semantik

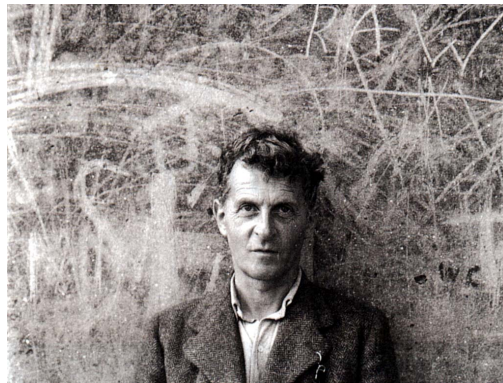
Folie 28

### Aussagen

*Die Frage „Was ist eigentlich ein Wort?“ ist analog der „Was ist eine Schachfigur?“* Ludwig Wittgenstein, *Philosophische Untersuchungen*

- *Aussagen* (im Sinne der Aussagenlogik) sind sprachliche Gebilde, die entweder *wahr* oder *falsch* sind.
- Aussagen können mit *Junktoren* wie *nicht*, *und*, *oder* oder *wenn ... dann* zu komplexeren Aussagen verknüpft werden.
- *Aussagenlogik* beschäftigt sich mit allgemeinen Prinzipien des korrekten Argumentierens und Schließens mit Aussagen und Kombinationen von Aussagen.

Folie 29



Ludwig Wittgenstein (1889 – 1951)

Quelle: [http://en.wikipedia.org/wiki/Ludwig\\_Wittgenstein](http://en.wikipedia.org/wiki/Ludwig_Wittgenstein)

Folie 30

**Beispiel 2.1** (Geburtstagsfeier).

Fred möchte mit möglichst vielen seiner Freunde Anne, Bernd, Christine, Dirk und Eva seinen Geburtstag feiern. Er weiß Folgendes:

Wenn Bernd und Anne beide zur Party kommen, dann wird Eva auf keinen Fall kommen. Und Dirk wird auf keinen Fall kommen, wenn Bernd und Eva beide zur Feier kommen. Aber Eva kommt allenfalls dann, wenn Christine und Dirk kommen. Andererseits kommt Christine nur dann, wenn auch Anne kommt. Anne wiederum wird nur dann kommen, wenn auch Bernd oder Christine dabei sind.

*Frage:* Wie viele Freunde (und welche) werden im besten Fall zur Party kommen?

Folie 31

Das Wissen, das in dem Text wiedergegeben ist, lässt sich in „*atomare Aussagen*“ zerlegen, die mit Junktoren verknüpft werden können.

Die atomaren Aussagen, um die sich der Text dreht, kürzen wir folgendermaßen ab:

- $A$  : Anne kommt zur Feier
- $B$  : Bernd kommt zur Feier
- $C$  : Christine kommt zur Feier
- $D$  : Dirk kommt zur Feier
- $E$  : Eva kommt zur Feier

Das im Text zusammengefasste Wissen lässt sich wie folgt repräsentieren.

Folie 32

- (1) Wenn Bernd und Anne beide zur Party kommen, dann wird Eva auf keinen Fall kommen.  
*kurz:* Wenn ( $B$  und  $A$ ), dann nicht  $E$       *kürzer:*  $(B \wedge A) \rightarrow \neg E$
- (2) Dirk wird auf keinen Fall kommen, wenn Bernd und Eva beide zur Feier kommen.  
*kurz:* Wenn ( $B$  und  $E$ ), dann nicht  $D$       *kürzer:*  $(B \wedge E) \rightarrow \neg D$
- (3) Eva kommt allenfalls dann, wenn Christine und Dirk kommen.  
*kurz:* Wenn  $E$ , dann ( $C$  und  $D$ )      *kürzer:*  $E \rightarrow (C \wedge D)$
- (4) Christine kommt nur dann, wenn auch Anne kommt.  
*kurz:* Wenn  $C$ , dann  $A$       *kürzer:*  $C \rightarrow A$
- (5) Anne kommt nur dann, wenn auch Bernd oder Christine dabei sind.  
*kurz:* Wenn  $A$ , dann ( $B$  oder  $C$ )      *kürzer:*  $A \rightarrow (B \vee C)$

Folie 33

### Fallstricke natürlichsprachlicher Aussagen

Die Verwendung der Wörter *und*, *wenn ... dann*, *oder*, *nicht* in der Alltagssprache entspricht nicht immer exakt unseren logischen Junktoren.

- (1) Anne hat mit dem Kaffeetrinken aufgehört.  
*kurz:*  $V$  und nicht  $G$       *kürzer:*  $V \wedge \neg G$
- (2) Anne hat *nicht* mit dem Kaffeetrinken aufgehört.  
*kurz:*  $V$  und  $G$       *kürzer:*  $V \wedge G$

Ist (2) die Negation von (1)? In dem Fall, dass Anne noch nie Kaffee getrunken hat, ist keine der beiden Aussagen wahr.

- $V$  : Anne war in der Vergangenheit Kaffeetrinkerin.  
 $G$  : Anne ist zur Zeit Kaffeetrinkerin.

Zwei weitere Beispiele:

- Ich werde mir ein rotes *oder* ein blaues Fahrrad kaufen.
- *Wenn* Regen vorhergesagt ist, *dann* nehme ich einen Schirm mit.

Folie 34

## Syntax und Semantik

**Syntax:** legt fest, welche Zeichenketten Formeln der Aussagenlogik sind

**Semantik:** legt fest, welche „Bedeutung“ einzelne Formeln haben

Dies ist analog zur Syntax und Semantik von Java-Programmen:

Die Syntax legt fest, welche Zeichenketten Java-Programme sind, während die Semantik bestimmt, was das Programm tut.

Zur Verdeutlichung werden wir im Folgenden **syntaktische Objekte** oft in **orange** darstellen, während wir **semantische Aussagen** in **blau** angeben.

### *Syntax der Aussagenlogik*

Folie 35

#### Notationen

- Die Menge  $\mathbb{N}$  der natürlichen Zahlen besteht aus allen nicht-negativen ganzen Zahlen, d.h.

$$\mathbb{N} := \{ 0, 1, 2, 3, \dots \}.$$

- Für ein  $n \in \mathbb{N}$  ist

$$[n] := \{1, \dots, n\} = \{ i \in \mathbb{N} : 1 \leq i \leq n \}.$$

Folie 36

**Definition 2.2.** Ein *Aussagensymbol* (oder eine *Aussagenvariable*, kurz: *Variable*) hat die Form  $A_i$  für ein  $i \in \mathbb{N}$ .

Die Menge aller Aussagensymbole bezeichnen wir mit **AS**, d.h.

$$\text{AS} = \{A_i : i \in \mathbb{N}\} = \{A_0, A_1, A_2, A_3, \dots\}$$

Aussagenlogische Formeln sind Wörter, die über dem folgenden Alphabet gebildet sind.

**Definition 2.3.** Das *Alphabet der Aussagenlogik* besteht aus

- den Aussagesymbolen in **AS**,



- den *Junktoren*  $\neg, \wedge, \vee, \rightarrow$ ,
- den *booleschen Konstanten*  $\mathbf{0}, \mathbf{1}$ ,
- den Klammersymbolen  $(, )$ .

Wir schreiben  $A_{\text{AL}}$ , um das Alphabet der Aussagenlogik zu bezeichnen, d.h.

$$A_{\text{AL}} := \text{AS} \cup \{ \neg, \wedge, \vee, \rightarrow, \mathbf{0}, \mathbf{1}, (, ) \}$$

**Bemerkung.** Wir haben hier festgelegt, dass es abzählbar unendlich viele Aussagensymbole gibt.

**Zur Erinnerung:**

Eine Menge  $M$  heißt *abzählbar unendlich*, wenn sie unendlich ist und ihre Elemente sich in der Form  $m_0, m_1, m_2, \dots$  aufzählen lassen. Formal heißt  $M$  genau dann *abzählbar unendlich*, wenn es eine bijektive Abbildung von der Menge  $\mathbb{N} = \{0, 1, 2, \dots\}$  der natürlichen Zahlen auf die Menge  $M$  gibt. Eine Menge  $M$  heißt *abzählbar*, wenn sie entweder endlich oder abzählbar unendlich ist. Eine Menge  $M$  heißt *überabzählbar*, wenn sie nicht abzählbar ist.

**Beispiele.** • Die Menge  $\mathbb{N}$  ist abzählbar unendlich.

- Ist  $A$  eine abzählbare Menge, so ist die Menge  $A^*$  aller endlichen Wörter über dem Alphabet  $A$  abzählbar. Ist etwa  $A = \{a_0, a_1, a_2, \dots\}$ , so können wir eine Aufzählung von  $A^*$  wie folgt beginnen:

$$\begin{aligned} &\varepsilon \quad (\text{das leere Wort}) \\ &a_0, \\ &a_1, a_0a_0, a_0a_1, a_1a_0, a_1a_1, \\ &a_2, a_0a_2, a_2a_0, a_1a_2, a_2a_1, a_2a_2, a_0a_0a_0, a_0a_0a_1, a_0a_0a_2, \dots, a_2a_2a_2 \\ &a_3, a_0a_3, \dots, a_3a_3a_3a_3, \\ &\dots \end{aligned}$$

- Die Menge  $\mathbb{R}$  aller reellen Zahlen ist überabzählbar.
- Ist  $M$  eine unendliche Menge, so ist die Potenzmenge  $\mathcal{P}(M) := 2^M := \{N \mid N \subseteq M\}$  von  $M$  überabzählbar.

**Bemerkung.** Wir könnten die Aussagenlogik genauso auf einer überabzählbaren Menge von Aussagensymbolen aufbauen. Alles würde genauso funktionieren, nur der Beweis des Endlichkeitssatzes (siehe Kapitel 2.5) würde komplizierter werden. Für die Anwendungen in der Informatik reicht allerdings i.d.R. eine abzählbar unendliche Menge.

Folie 37

**Definition 2.4** (Syntax der Aussagenlogik).

Die Menge  $AL$  der *aussagenlogischen Formeln* (kurz: *Formeln*) ist die folgendermaßen rekursiv definierte Teilmenge von  $A_{AL}^*$ :

*Basisregeln:* (zum Bilden der so genannten *atomaren Formeln*)

$$(B0) \mathbf{0} \in AL$$

$$(B1) \mathbf{1} \in AL$$

$$(BS) \text{ Für jedes Aussagensymbol } A_i \in AS \text{ gilt: } A_i \in AL$$

*Rekursive Regeln:*

$$(R1) \text{ Ist } \varphi \in AL, \text{ so ist auch } \neg\varphi \in AL \text{ (Negation)}$$

$$(R2) \text{ Ist } \varphi \in AL \text{ und } \psi \in AL, \text{ so ist auch}$$

- $(\varphi \wedge \psi) \in AL$  (Konjunktion)
- $(\varphi \vee \psi) \in AL$  (Disjunktion)
- $(\varphi \rightarrow \psi) \in AL$  (Implikation)

Folie 38

### Beispiele

- $(\neg A_0 \vee (A_0 \rightarrow A_1)) \in AL$
- $\neg((A_0 \wedge \mathbf{0}) \rightarrow \neg A_3) \in AL$
- $A_1 \vee A_2 \wedge A_3 \notin AL$
- $(\neg A_1) \notin AL$

Folie 39

## Griechische Buchstaben

In der Literatur werden Formeln einer Logik traditionell meistens mit griechischen Buchstaben bezeichnet.

Hier eine Liste der gebräuchlichsten Buchstaben:

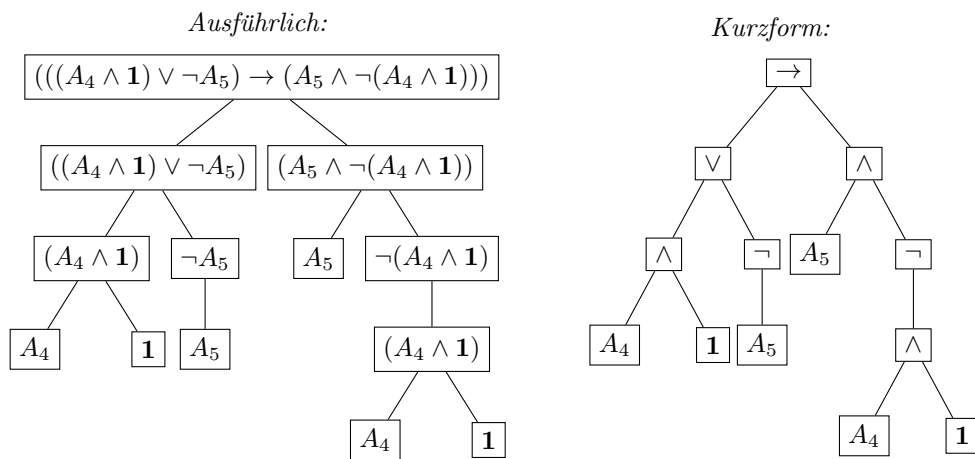
Buchstabe	$\varphi$	$\psi$	$\chi$	$\theta$ bzw. $\vartheta$	$\lambda$	$\mu$	$\nu$	$\tau$	$\kappa$
Aussprache	phi	psi	chi	theta	lambda	mü	nü	tau	kappa
Buchstabe	$\sigma$	$\rho$	$\xi$	$\zeta$	$\alpha$	$\beta$	$\gamma$	$\delta$	$\omega$
Aussprache	sigma	rho	xi	zeta	alpha	beta	gamma	delta	omega
Buchstabe	$\varepsilon$	$\iota$	$\pi$	$\Delta$	$\Gamma$	$\Sigma$	$\Pi$	$\Phi$	$\Psi$
Aussprache	epsilon	iota	pi	Delta	Gamma	Sigma	Pi	Phi	Psi

Folie 40

## Syntaxbäume

Die Struktur einer Formel lässt sich bequem in einem *Syntaxbaum* (englisch: *parse tree*) darstellen.

*Beispiel:* Syntaxbaum der Formel  $((A_4 \wedge \mathbf{1}) \vee \neg A_5) \rightarrow (A_5 \wedge \neg(A_4 \wedge \mathbf{1}))$



Folie 41

## Subformeln und eindeutige Lesbarkeit

- Jede Formel hat genau einen Syntaxbaum. Diese Aussage ist als das *Lemma über die eindeutige Lesbarkeit aussagenlogischer Formeln* bekannt.

- Die Formeln  $\psi$ , die im ausführlichen Syntaxbaum einer Formel  $\varphi$  als Knotenbeschriftung vorkommen, nennen wir *Subformeln* (bzw. *Teilformeln*) von  $\varphi$ .
- Eine Subformel  $\psi$  von  $\varphi$  kann an mehreren Knoten des Syntaxbaums vorkommen. Wir sprechen dann von verschiedenen *Vorkommen* von  $\psi$  in  $\varphi$ .

## *Semantik der Aussagenlogik*

Folie 42

### Vorüberlegung zur Semantik

- Eine aussagenlogische Formel wird erst zur Aussage, wenn wir alle in ihr vorkommenden **Aussagensymbole** durch **Aussagen** ersetzen.
- Wir interessieren uns hier nicht so sehr für die tatsächlichen Aussagen, sondern nur für ihren **Wahrheitswert**, also dafür, ob sie wahr oder falsch sind.
- Um das festzustellen, reicht es, den Aussagensymbolen die Wahrheitswerte der durch sie repräsentierten Aussagen zuzuordnen.
- *Die Bedeutung einer Formel besteht also aus ihren Wahrheitswerten unter allen möglichen Wahrheitswerten für die in der Formel vorkommenden Aussagensymbole.*

Folie 43

### Interpretationen (d.h. Variablenbelegungen)

Wir repräsentieren die Wahrheitswerte **wahr** und **falsch** durch **1** und **0**.

**Definition 2.5.** Eine **aussagenlogische Interpretation** (kurz: **Interpretation** oder **Belegung**) ist eine Abbildung

$$\mathcal{I} : \text{AS} \rightarrow \{0, 1\}.$$

D.h.:  $\mathcal{I}$  „belegt“ jedes Aussagensymbol  $X \in \text{AS}$  mit einem der beiden Wahrheitswerte 1 (für „wahr“) oder 0 (für „falsch“); und  $\mathcal{I}(X)$  ist der Wahrheitswert, mit dem das Aussagensymbol  $X$  belegt wird.

Folie 44

## Semantik der Aussagenlogik

**Definition 2.6.** Zu jeder Formel  $\varphi \in \text{AL}$  und jeder Interpretation  $\mathcal{I}$  definieren wir einen **Wahrheitswert**  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  rekursiv wie folgt:

*Rekursionsanfang:*

- $\llbracket \mathbf{0} \rrbracket^{\mathcal{I}} := 0$ .
- $\llbracket \mathbf{1} \rrbracket^{\mathcal{I}} := 1$ .
- Für alle  $X \in \text{AS}$  gilt:  $\llbracket X \rrbracket^{\mathcal{I}} := \mathcal{I}(X)$ .

*Rekursionsschritt:*

- Ist  $\varphi \in \text{AL}$ , so ist  $\llbracket \neg \varphi \rrbracket^{\mathcal{I}} := \begin{cases} 1 & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 0, \\ 0 & \text{sonst.} \end{cases}$

Folie 45

- Ist  $\varphi \in \text{AL}$  und  $\psi \in \text{AL}$ , so ist

$$\begin{aligned}
 - \llbracket (\varphi \wedge \psi) \rrbracket^{\mathcal{I}} &:= \begin{cases} 1 & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = \llbracket \psi \rrbracket^{\mathcal{I}} = 1, \\ 0 & \text{sonst.} \end{cases} \\
 - \llbracket (\varphi \vee \psi) \rrbracket^{\mathcal{I}} &:= \begin{cases} 0 & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = \llbracket \psi \rrbracket^{\mathcal{I}} = 0, \\ 1 & \text{sonst.} \end{cases} \\
 - \llbracket (\varphi \rightarrow \psi) \rrbracket^{\mathcal{I}} &:= \begin{cases} 0 & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 1 \text{ und } \llbracket \psi \rrbracket^{\mathcal{I}} = 0, \\ 1 & \text{sonst.} \end{cases}
 \end{aligned}$$

Folie 46

## Intuitive Bedeutung der Semantik

**Boolesche Konstanten:**  $\mathbf{1}$  und  $\mathbf{0}$  bedeuten einfach „*wahr*“ und „*falsch*“.

**Aussagensymbole:** Die Aussagensymbole stehen für irgendwelche Aussagen, von denen uns aber nur der Wahrheitswert interessiert. Dieser wird durch die Interpretation festgelegt.

**Negation:**  $\neg \varphi$  bedeutet „*nicht*  $\varphi$ “.

**Konjunktion:**  $(\varphi \wedge \psi)$  bedeutet „ $\varphi$  und  $\psi$ “.

**Disjunktion:**  $(\varphi \vee \psi)$  bedeutet „ $\varphi$  oder  $\psi$ “.

**Implikation:**  $(\varphi \rightarrow \psi)$  bedeutet „ $\varphi$  impliziert  $\psi$ “ (oder „wenn  $\varphi$  dann  $\psi$ “).

Folie 47

## Rekursive Definitionen über Formeln

- Ähnlich wie Funktionen auf den natürlichen Zahlen, wie zum Beispiel die Fakultätsfunktion oder die Fibonacci Folge, können wir Funktionen auf den aussagenlogischen Formeln rekursiv definieren.
- Dabei gehen wir von den atomaren Formeln aus und definieren dann den Funktionswert einer zusammengesetzten Formel aus den Funktionswerten ihrer Bestandteile.
- Zur Rechtfertigung solcher Definitionen benötigt man die eindeutige Lesbarkeit aussagenlogischer Formeln, die besagt, dass sich jede Formel eindeutig in ihre Bestandteile zerlegen lässt.
- Wir haben auf diese Weise die Semantik definiert. Wir haben nämlich für jede Interpretation  $\mathcal{I}$  rekursiv eine Funktion  $\llbracket \cdot \rrbracket^{\mathcal{I}} : \text{AL} \rightarrow \{0, 1\}$  definiert.

Folie 48

Schematisch sieht die rekursive Definition einer Funktion  $f : \text{AL} \rightarrow M$  (für eine beliebige Menge  $M$ ) folgendermaßen aus:

*Rekursionsanfang:*

- Definiere  $f(\mathbf{0})$  und  $f(\mathbf{1})$ .
- Definiere  $f(X)$  für alle  $X \in \text{AS}$ .

*Rekursionsschritt:*

- Definiere  $f(\neg\varphi)$  aus  $f(\varphi)$ .
- Definiere  $f((\varphi \wedge \psi))$  aus  $f(\varphi)$  und  $f(\psi)$ .
- Definiere  $f((\varphi \vee \psi))$  aus  $f(\varphi)$  und  $f(\psi)$ .

- Definiere  $f((\varphi \rightarrow \psi))$  aus  $f(\varphi)$  und  $f(\psi)$ .

Folie 49

**Beispiel 2.7.**

Betrachte die Formel  $\varphi := (\neg A_0 \vee (A_5 \rightarrow A_1))$

und die Interpretation  $\mathcal{I} : \text{AS} \rightarrow \{0, 1\}$  mit

$$\mathcal{I}(A_0) = 1, \quad \mathcal{I}(A_1) = 1, \quad \mathcal{I}(A_5) = 0$$

und  $\mathcal{I}(Y) = 0$  für alle  $Y \in \text{AS} \setminus \{A_0, A_1, A_5\}$ .

Der Wahrheitswert  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  ist der Wert

$$\begin{aligned} \llbracket \varphi \rrbracket^{\mathcal{I}} &\stackrel{\text{Def. 2.6}}{=} \begin{cases} 0, & \text{falls } \llbracket \neg A_0 \rrbracket^{\mathcal{I}} = 0 \text{ und } \llbracket (A_5 \rightarrow A_1) \rrbracket^{\mathcal{I}} = 0 \\ 1, & \text{sonst} \end{cases} \\ &\stackrel{\text{Def. 2.6}}{=} \begin{cases} 0, & \text{falls } \llbracket A_0 \rrbracket^{\mathcal{I}} = 1 \text{ und } (\llbracket A_5 \rrbracket^{\mathcal{I}} = 1 \text{ und } \llbracket A_1 \rrbracket^{\mathcal{I}} = 0) \\ 1, & \text{sonst} \end{cases} \\ &\stackrel{\text{Def. 2.6}}{=} \begin{cases} 0, & \text{falls } \mathcal{I}(A_0) = 1 \text{ und } \mathcal{I}(A_5) = 1 \text{ und } \mathcal{I}(A_1) = 0 \\ 1, & \text{sonst} \end{cases} \\ &= 1 \quad (\text{denn gemäß obiger Wahl von } \mathcal{I} \text{ gilt } \mathcal{I}(A_5) = 0). \end{aligned}$$

Folie 50

**Alternative Art, den Wert  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  zu bestimmen**

- Ersetze in  $\varphi$  jedes Aussagensymbol  $X$  durch seinen gemäß  $\mathcal{I}$  festgelegten Wahrheitswert, d.h. durch den Wert  $\mathcal{I}(X)$ , und rechne dann den Wert des resultierenden booleschen Ausdrucks aus.
- Speziell für die Formel  $\varphi$  und die Interpretation  $\mathcal{I}$  aus Beispiel 2.7 ergibt die Ersetzung der Aussagensymbole durch die gemäß  $\mathcal{I}$  festgelegten Wahrheitswerte den booleschen Ausdruck

$$(\neg 1 \vee (0 \rightarrow 1)).$$

- Ausrechnen von  $\neg 1$  ergibt den Wert 0.  
Ausrechnen von  $(0 \rightarrow 1)$  ergibt den Wert 1.
- Insgesamt erhalten wir also  $(0 \vee 1)$ , was sich zum Wert 1 errechnet.  
Somit erhalten wir, dass  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 1$  ist.

Folie 51

## Die Modellbeziehung

### Definition 2.8.

- (a) Eine Interpretation  $\mathcal{I}$  erfüllt eine Formel  $\varphi \in \mathbf{AL}$  (wir schreiben:  $\mathcal{I} \models \varphi$ ), wenn  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 1$ .  
Wir schreiben kurz  $\mathcal{I} \not\models \varphi$  um auszudrücken, dass  $\mathcal{I}$  die Formel  $\varphi$  nicht erfüllt (d.h., es gilt  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 0$ ).
- (b) Eine Interpretation  $\mathcal{I}$  erfüllt eine Formelmenge  $\Phi \subseteq \mathbf{AL}$  (wir schreiben:  $\mathcal{I} \models \Phi$ ), wenn  $\mathcal{I} \models \varphi$  für alle  $\varphi \in \Phi$ .
- (c) Ein Modell einer Formel  $\varphi$  (bzw. einer Formelmenge  $\Phi$ ) ist eine Interpretation  $\mathcal{I}$  mit  $\mathcal{I} \models \varphi$  (bzw.  $\mathcal{I} \models \Phi$ ).

Folie 52

## Das Koinzidenzlemma

- Offensichtlich hängt der Wert  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  nur von den Werten  $\mathcal{I}(X)$  der Aussagensymbole  $X \in \mathbf{AS}$  ab, die auch in  $\varphi$  vorkommen.  
Diese Aussage ist als das *Koinzidenzlemma der Aussagenlogik* bekannt.
- Um  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  festzulegen, reicht es also, die Werte  $\mathcal{I}(X)$  nur für diejenigen Aussagensymbole  $X \in \mathbf{AS}$  anzugeben, die in  $\varphi$  vorkommen.

Folie 53

## Vereinbarungen zu Interpretationen

- Statt der vollen Interpretation  $\mathcal{I} : \mathbf{AS} \rightarrow \{0, 1\}$  geben wir in der Regel nur endlich viele Werte  $\mathcal{I}(X_1), \dots, \mathcal{I}(X_n)$  an und legen fest, dass  $\mathcal{I}(Y) := 0$  für alle  $Y \in \mathbf{AS} \setminus \{X_1, \dots, X_n\}$ .
- In den Beispielen legen wir eine Interpretation oft durch eine Wertetabelle fest. Beispielsweise beschreibt die Tabelle

$X$	$A_0$	$A_1$	$A_5$
$\mathcal{I}(X)$	1	1	0

die Interpretation  $\mathcal{I}$  mit  $\mathcal{I}(A_0) = \mathcal{I}(A_1) = 1$  und  $\mathcal{I}(A_5) = 0$  und  $\mathcal{I}(Y) = 0$  für alle  $Y \in \mathbf{AS} \setminus \{A_0, A_1, A_5\}$ .



- Wir schreiben  $\varphi(X_1, \dots, X_n)$ , um anzudeuten, dass in  $\varphi$  nur Aussagensymbole aus der Menge  $\{X_1, \dots, X_n\}$  vorkommen.  
Für Wahrheitswerte  $b_1, \dots, b_n \in \{0, 1\}$  schreiben wir dann  $\varphi[b_1, \dots, b_n]$  anstatt  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  für eine (bzw. alle) Interpretationen  $\mathcal{I}$  mit  $\mathcal{I}(X_i) = b_i$  für alle  $i \in [n] := \{1, \dots, n\}$ .

Folie 54

## Vereinbarungen

- Wir schreiben  $(\varphi \leftrightarrow \psi)$  als Abkürzung für  $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$ .
- Statt mit  $A_0, A_1, A_2, \dots$  bezeichnen wir *Aussagensymbole* auch oft mit  $A, B, C, \dots, X, Y, Z, \dots$  oder mit Varianten wie  $X', Y_1, \dots$ .
- Die äußeren Klammern einer Formel lassen wir manchmal weg und schreiben z.B.  $(X \wedge Y) \rightarrow Z$  an Stelle des (formal korrekten)  $((X \wedge Y) \rightarrow Z)$ .
- Bezüglich Klammerung vereinbaren wir, dass  $\neg$  am stärksten bindet, und dass  $\wedge$  und  $\vee$  stärker binden als  $\rightarrow$ .

Wir können also z.B.  $X \wedge \neg Y \rightarrow Z \vee X$  schreiben und meinen damit

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

Nicht schreiben können wir z.B.  $X \wedge Y \vee Z$  (da wir nichts darüber vereinbart haben, wie fehlende Klammern hier zu setzen sind).

Folie 55

- Wir schreiben  $\bigwedge_{i=1}^n \varphi_i$  bzw.  $(\varphi_1 \wedge \dots \wedge \varphi_n)$  an Stelle von

$$(\dots((\varphi_1 \wedge \varphi_2) \wedge \varphi_3) \wedge \dots \wedge \varphi_n)$$

und nutzen analoge Schreibweisen auch für „ $\vee$ “ an Stelle von „ $\wedge$ “.

- Ist  $M$  eine *endliche, nicht-leere* Menge aussagenlogischer Formeln, so schreiben wir

$$\bigwedge_{\varphi \in M} \varphi$$

um die Formel  $(\varphi_1 \wedge \dots \wedge \varphi_n)$  zu bezeichnen, wobei  $n = |M|$  die Anzahl der Formeln in  $M$  ist und  $\varphi_1, \dots, \varphi_n$  die Auflistung aller Formeln in  $M$  in lexikographischer Reihenfolge ist. Formeln sind hierbei Worte über dem Alphabet der Aussagenlogik, wobei die einzelnen Symbole dieses Alphabets folgendermaßen aufsteigend sortiert sind:

$$0, 1, \neg, \wedge, \vee, \rightarrow, (, ), A_0, A_1, A_2, A_3, \dots$$

Die analoge Schreibweise nutzen wir auch für „ $\vee$ “ an Stelle von „ $\wedge$ “.

Folie 56

- Diese Schreibweisen werden wir manchmal auch kombinieren. Sind zum Beispiel  $I = \{i_1, \dots, i_m\}$  und  $J = \{j_1, \dots, j_n\}$  endliche Mengen und ist für jedes  $i \in I$  und  $j \in J$  eine Formel  $\varphi_{i,j}$  gegeben, so schreiben wir

$$\bigwedge_{i \in I} \bigvee_{j \in J} \varphi_{i,j}$$

um die Formel  $(\psi_{i_1} \wedge \dots \wedge \psi_{i_m})$  zu bezeichnen, wobei für jedes  $i \in I$  die Formel  $\psi_i$  durch  $\psi_i := (\varphi_{i,j_1} \vee \dots \vee \varphi_{i,j_n})$  definiert ist.

Folie 57

## Wahrheitstafeln

Für jede Formel  $\varphi(X_1, \dots, X_n)$  kann man die **Wahrheitswerte unter allen möglichen Interpretationen** in einer **Wahrheitstafel** darstellen. Für alle  $(b_1, \dots, b_n) \in \{0, 1\}^n$  enthält die Tafel eine Zeile mit den Werten  $b_1 \dots b_n \mid \varphi[b_1, \dots, b_n]$ .

Um die Wahrheitstafel für  $\varphi$  auszufüllen, ist es bequem, auch Spalten für (alle oder einige) Subformeln von  $\varphi$  einzufügen.

*Beispiel:* Wahrheitstafel für  $\varphi(X, Y, Z) := ((X \vee Y) \rightarrow (X \wedge Z))$ :

$X$	$Y$	$Z$	$(X \vee Y)$	$(X \wedge Z)$	$\varphi$
0	0	0	0	0	1
0	0	1	0	0	1
0	1	0	1	0	0
0	1	1	1	0	0
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	1	0	0
1	1	1	1	1	1

Die Reihenfolge der Zeilen ist dabei unerheblich. Wir vereinbaren allerdings, die Zeilen stets so anzuordnen, dass die Werte  $b_1 \cdots b_n \in \{0, 1\}^n$ , aufgefasst als Binärzahlen, in aufsteigender Reihenfolge aufgelistet werden.

Folie 58

## Wahrheitstafeln für die Junktoren

Die Bedeutung der Junktoren kann man mittels ihrer Wahrheitstafeln beschreiben:

$X$	$\neg X$	$X$	$Y$	$(X \wedge Y)$	$X$	$Y$	$(X \vee Y)$	$X$	$Y$	$(X \rightarrow Y)$
0	1	0	0	0	0	0	0	0	0	1
0	1	0	1	0	0	1	1	0	1	1
1	0	1	0	0	1	0	1	1	0	0
1	0	1	1	1	1	1	1	1	1	1

Genauso kann man eine Wahrheitstafel für die Formel  $X \leftrightarrow Y$ , die ja eine Abkürzung für  $(X \rightarrow Y) \wedge (Y \rightarrow X)$  ist, bestimmen:

$X$	$Y$	$(X \leftrightarrow Y)$
0	0	1
0	1	0
1	0	0
1	1	1

$X \leftrightarrow Y$  bedeutet also „ $X$  genau dann wenn  $Y$ “.

Folie 59

## Ein Logikrätsel

**Beispiel 2.9.** Auf der Insel Wafa gibt es zwei Dörfer: Das Dorf Wa, dessen Einwohner:innen immer die Wahrheit sagen, und das Dorf Fa, dessen Einwohner:innen immer lügen. Ein Reisender besucht die Insel und trifft auf drei Einwohner  $A$ ,  $B$ ,  $C$ , die ihm Folgendes erzählen:

- $A$  sagt:  
„ $B$  und  $C$  sagen genau dann die Wahrheit, wenn  $C$  die Wahrheit sagt.“
- $B$  sagt:  
„Wenn  $A$  und  $C$  die Wahrheit sagen, dann ist es nicht der Fall, dass  $A$  die Wahrheit sagt, wenn  $B$  und  $C$  die Wahrheit sagen.“

- $C$  sagt:  
*„ $B$  lügt genau dann, wenn  $A$  oder  $B$  die Wahrheit sagen.“*

*Frage:* In welchen der beiden Dörfern leben jeweils  $A$ ,  $B$  bzw.  $C$ ?

Folie 60

## Aussagenlogische Modellierung

Aussagensymbole:

- $W_A$  steht für „ $A$  sagt die Wahrheit.“
- $W_B$  steht für „ $B$  sagt die Wahrheit.“
- $W_C$  steht für „ $C$  sagt die Wahrheit.“

Aussagen der drei Inselbewohner:

- $\varphi_A := (W_B \wedge W_C) \leftrightarrow W_C$
- $\varphi_B := (W_A \wedge W_C) \rightarrow \neg((W_B \wedge W_C) \rightarrow W_A)$
- $\varphi_C := \neg W_B \leftrightarrow (W_A \vee W_B)$

Wir suchen nach einer Interpretation, die die Formel

$$\psi := (W_A \leftrightarrow \varphi_A) \wedge (W_B \leftrightarrow \varphi_B) \wedge (W_C \leftrightarrow \varphi_C)$$

erfüllt.

Folie 61

## Lösung mittels Wahrheitstafel

$W_A$	$W_B$	$W_C$	$\varphi_A$	$\varphi_B$	$\varphi_C$	$W_A \leftrightarrow \varphi_A$	$W_B \leftrightarrow \varphi_B$	$W_C \leftrightarrow \varphi_C$	$\psi$
0	0	0	1	1	0	0	0	1	0
0	0	1	0	1	0	1	0	0	0
0	1	0	1	1	0	0	1	1	0
0	1	1	1	1	0	0	1	0	0
1	0	0	1	1	1	1	0	0	0
1	0	1	0	0	1	0	1	1	0
1	1	0	1	1	0	1	1	1	1
1	1	1	1	0	0	1	0	0	0

Die Interpretation  $\mathcal{I}$  mit  $\mathcal{I}(W_A) = 1$ ,  $\mathcal{I}(W_B) = 1$ ,  $\mathcal{I}(W_C) = 0$  in Zeile 7 ist die einzige, die die Formel  $\psi$  erfüllt.

Gemäß dieser Interpretation sind die Aussagen, die durch die Symbole  $W_A$  und  $W_B$  repräsentiert werden, wahr, während die Aussage, die durch  $W_C$  repräsentiert wird, falsch ist.

Das heißt, die Personen  $A$  und  $B$  sagen die Wahrheit und leben somit im Dorf Wa, und Person  $C$  lügt und lebt daher im Dorf Fa.

Folie 62

## Computerlesbare Darstellung von Formeln

Wir betrachten das Alphabet **ASCII** aller ASCII-Symbole.

Die Menge  $\mathbf{AS}_{\text{ASCII}}$  aller ASCII-Repräsentationen von Aussagensymbolen besteht aus allen nicht-leeren Worten über dem Alphabet **ASCII**, deren erstes Symbol ein Buchstabe ist, und bei dem alle weiteren Symbole Buchstaben oder Ziffern sind.

Die Menge  $\mathbf{AL}_{\text{ASCII}}$  aller ASCII-Repräsentationen von aussagenlogischen Formeln ist die rekursiv wie folgt definierte Teilmenge von  $\mathbf{ASCII}^*$ :

*Basisregeln:*

- $0 \in \mathbf{AL}_{\text{ASCII}}$ ,  $1 \in \mathbf{AL}_{\text{ASCII}}$  und  $w \in \mathbf{AL}_{\text{ASCII}}$  für alle  $w \in \mathbf{AS}_{\text{ASCII}}$ .

*Rekursive Regeln:*

- Ist  $\varphi \in \mathbf{AL}_{\text{ASCII}}$ , so ist auch  $\sim\varphi \in \mathbf{AL}_{\text{ASCII}}$ . (*Negation*)
- Ist  $\varphi \in \mathbf{AL}_{\text{ASCII}}$  und  $\psi \in \mathbf{AL}_{\text{ASCII}}$ , so ist auch
  - $(\varphi \wedge \psi) \in \mathbf{AL}_{\text{ASCII}}$  (*Konjunktion*)
  - $(\varphi \vee \psi) \in \mathbf{AL}_{\text{ASCII}}$  (*Disjunktion*)
  - $(\varphi \rightarrow \psi) \in \mathbf{AL}_{\text{ASCII}}$  (*Implikation*)
  - $(\varphi \leftrightarrow \psi) \in \mathbf{AL}_{\text{ASCII}}$  (*Bimplikation*).

Folie 63

## Abstrakte vs. computerlesbare Syntax

Es ist offensichtlich, wie man Formeln aus AL in ihre entsprechende ASCII-Repräsentation übersetzt und umgekehrt. Zum Beispiel ist

$$((A_0 \wedge 0) \rightarrow \neg A_{13})$$

eine Formel in AL, deren ASCII-Repräsentation die folgende Zeichenkette aus  $AL_{ASCII}$  ist:

$$( (A0/\wedge 0) -> \sim A13 ).$$

Wir werden meistens mit der „abstrakten Syntax“, d.h. mit der in Definition 2.4 festgelegten Menge AL, arbeiten. Um aber Formeln in Computer-Programme einzugeben, können wir die ASCII-Repräsentation verwenden.

Folie 64

### Demo: snippets of logic

- ein Formelchecker für die Aussagenlogik
- entwickelt von André Frochaux
- Funktionalitäten u.a.:
  - Syntaxcheck für eingegebene Formeln
  - Ausgabe eines Syntaxbaums
  - Ausgabe einer Wahrheitstafel
- Zugänglich via

[http://www.snippets-of-logic.net/index\\_AL.php?lang=de](http://www.snippets-of-logic.net/index_AL.php?lang=de)

Folie 65

### Zurück zu Beispiel 2.1 („Geburtstagsfeier“)

Das in Beispiel 2.1 aufgelistete Wissen kann durch folgende aussagenlogische Formel repräsentiert werden:

$$\begin{aligned}\varphi := & ((B \wedge A) \rightarrow \neg E) \wedge ((B \wedge E) \rightarrow \neg D) \wedge \\ & (E \rightarrow (C \wedge D)) \wedge (C \rightarrow A) \wedge (A \rightarrow (B \vee C))\end{aligned}$$

Die Frage

*„Wie viele (und welche) Freunde werden im besten Fall zur Party kommen?“*

kann nun durch Lösen der folgenden Aufgabe beantwortet werden:

Finde eine Interpretation  $\mathcal{I}$  für  $\varphi$ , so dass gilt:

- $\mathcal{I} \models \varphi$  (d.h.,  $\mathcal{I}$  ist ein *Modell* von  $\varphi$ ) und
- $|\{X \in \{A, B, C, D, E\} : \mathcal{I}(X) = 1\}|$  ist so groß wie möglich.

Folie 66

Diese Frage können wir lösen, indem wir

- (1) die Wahrheitstafel für  $\varphi$  ermitteln,
- (2) alle Zeilen raussuchen, in denen in der mit „ $\varphi$ “ beschrifteten Spalte der Wert 1 steht (das liefert uns genau die Modelle von  $\varphi$ ) und
- (3) aus diesen Zeilen all jene raussuchen, bei denen in den mit  $A, B, C, D, E$  beschrifteten Spalten möglichst viele Einsen stehen. Jede dieser Zeilen repräsentiert dann eine größtmögliche Konstellation von gleichzeitigen Partybesuchern.

Prinzipiell führt diese Vorgehensweise zum Ziel.

Leider ist das Verfahren aber recht aufwändig, da die Wahrheitstafel, die man dabei aufstellen muss, sehr groß wird: Sie hat  $2^5 = 32$  Zeilen.

Folie 67

$A$	$B$	$C$	$D$	$E$	$E \rightarrow (C \wedge D)$	$C \rightarrow A$	$(B \wedge E) \rightarrow \neg D$	$A \rightarrow (B \vee C)$	$(B \wedge A) \rightarrow \neg E$	$\varphi$
0	0	0	0	0	1	1	1	1	1	1
0	0	0	0	1	0	1	1	1	1	0
0	0	0	1	0	1	1	1	1	1	1
0	0	0	1	1	0	1	1	1	1	0
0	0	1	0	0	1	0	1	1	1	0
0	0	1	0	1	0	0	1	1	1	0
0	0	1	1	0	1	0	1	1	1	0
0	0	1	1	1	1	0	1	1	1	0
0	1	0	0	0	1	1	1	1	1	1
0	1	0	0	1	0	1	1	1	1	0
0	1	0	1	0	1	1	1	1	1	1
0	1	0	1	1	0	1	0	1	1	0
0	1	1	0	0	1	0	1	1	1	0
0	1	1	0	1	0	0	1	1	1	0
0	1	1	1	0	1	0	1	1	1	0
0	1	1	1	1	1	0	0	1	1	0
1	0	0	0	0	1	1	1	0	1	0
1	0	0	0	1	0	1	1	0	1	0
1	0	0	1	0	1	1	1	0	1	0
1	0	0	1	1	0	1	1	0	1	0
1	0	1	0	0	1	1	1	1	1	1
1	0	1	0	1	0	1	1	1	1	0
1	0	1	1	0	1	1	1	1	1	1
1	0	1	1	1	1	1	1	1	1	1
1	1	0	0	0	1	1	1	1	1	1
1	1	0	0	1	0	1	1	1	0	0
1	1	0	1	0	1	1	1	1	1	1
1	1	0	1	1	0	1	0	1	0	0
1	1	1	0	0	1	1	1	1	1	1
1	1	1	0	1	0	1	1	1	0	0
1	1	1	1	0	1	1	1	1	1	1
1	1	1	1	1	1	1	0	1	0	0

Folie 68

In der Wahrheitstafel sieht man:

- Es gibt *kein* Modell für  $\varphi$ , bei dem in den mit  $A$  bis  $E$  beschrifteten Spalten insgesamt 5 Einsen stehen.
- Es gibt genau *zwei* Modelle für  $\varphi$ , bei denen in den mit  $A$  bis  $E$  beschrifteten Spalten insgesamt 4 Einsen stehen, nämlich die beiden Interpretationen  $\mathcal{I}_1$  und  $\mathcal{I}_2$  mit

$$\mathcal{I}_1(A) = \mathcal{I}_1(C) = \mathcal{I}_1(D) = \mathcal{I}_1(E) = 1 \quad \text{und} \quad \mathcal{I}_1(B) = 0$$

und

$$\mathcal{I}_2(A) = \mathcal{I}_2(B) = \mathcal{I}_2(C) = \mathcal{I}_2(D) = 1 \quad \text{und} \quad \mathcal{I}_2(E) = 0.$$

Die Antwort auf die Frage „Wie viele (und welche) Freunde werden bestenfalls zur Party kommen?“ lautet also:

Bestenfalls werden 4 der 5 Freunde kommen, und dafür gibt es zwei Möglichkeiten, nämlich



- (1) dass alle außer Bernd kommen, und
- (2) dass alle außer Eva kommen.

## *Erfüllbarkeit, Allgemeingültigkeit und die Folgerungsbeziehung*

Folie 69

### **Erfüllbarkeit**

#### **Definition 2.10.**

Eine Formel  $\varphi \in \text{AL}$  heißt *erfüllbar*, wenn es eine Interpretation gibt, die  $\varphi$  erfüllt.

Eine Formelmenge  $\Phi$  heißt *erfüllbar*, wenn es eine Interpretation  $\mathcal{I}$  gibt, die  $\Phi$  erfüllt (d.h. es gilt  $\mathcal{I} \models \varphi$  für jedes  $\varphi \in \Phi$ ).

Eine Formel oder Formelmenge, die nicht erfüllbar ist, nennen wir *unerfüllbar*.

#### **Beobachtung 2.11.**

- (a) *Eine aussagenlogische Formel ist genau dann erfüllbar, wenn in der letzten Spalte ihrer Wahrheitstafel mindestens eine 1 steht.*
- (b) *Eine endliche Formelmenge  $\Phi = \{\varphi_1, \dots, \varphi_n\}$  ist genau dann erfüllbar, wenn die Formel  $\bigwedge_{i=1}^n \varphi_i$  erfüllbar ist.*

*Beispiele:*

- Die Formel  $X$  ist erfüllbar.
- Die Formel  $(X \wedge \neg X)$  ist unerfüllbar.

Folie 70

### **Allgemeingültigkeit**

**Definition 2.12.** Eine Formel  $\varphi \in \text{AL}$  ist *allgemeingültig*, wenn jede Interpretation  $\mathcal{I}$  die Formel  $\varphi$  erfüllt.

**Bemerkung.** Allgemeingültige Formeln nennt man auch *Tautologien*.

Man schreibt auch  $\models \varphi$  um auszudrücken, dass  $\varphi$  allgemeingültig ist.

**Beobachtung 2.13.**

*Eine aussagenlogische Formel ist genau dann allgemeingültig, wenn in der letzten Spalte ihrer Wahrheitstafel nur 1en stehen.*

*Beispiel:* Die Formel  $(X \vee \neg X)$  ist allgemeingültig.

Folie 71

**Beispiel 2.14.** Die Formel  $(X \vee Y) \wedge (\neg X \vee Y)$  ist

- *erfüllbar*, da z.B. die Interpretation  $\mathcal{I}$  mit  $\mathcal{I}(X) = 0$  und  $\mathcal{I}(Y) = 1$  die Formel erfüllt.
- *nicht allgemeingültig*, da z.B. die Interpretation  $\mathcal{I}'$  mit  $\mathcal{I}'(X) = 0$  und  $\mathcal{I}'(Y) = 0$  die Formel nicht erfüllt.

Folie 72

**Die Folgerungsbeziehung**

**Definition 2.15.** Eine Formel  $\psi \in \text{AL}$  folgt aus einer Formelmenge  $\Phi \subseteq \text{AL}$  (wir schreiben:  $\Phi \models \psi$ ), wenn für jede Interpretation  $\mathcal{I}$  gilt: Wenn  $\mathcal{I}$  die Formelmenge  $\Phi$  erfüllt, dann erfüllt  $\mathcal{I}$  auch die Formel  $\psi$ .

**Notation.** Für zwei Formeln  $\varphi, \psi \in \text{AL}$  schreiben wir kurz  $\varphi \models \psi$  an Stelle von  $\{\varphi\} \models \psi$  und sagen, dass die Formel  $\psi$  aus der Formel  $\varphi$  folgt.

Folie 73

**Beispiel 2.16.** Sei  $\varphi := ((X \vee Y) \wedge (\neg X \vee Y))$  und  $\psi := (Y \vee (\neg X \wedge \neg Y))$ .

Dann gilt  $\varphi \models \psi$ , aber es gilt *nicht*  $\psi \models \varphi$  (kurz:  $\psi \not\models \varphi$ ), denn:

$X$	$Y$	$(X \vee Y)$	$(\neg X \vee Y)$	$\varphi$	$\psi$
0	0	0	1	0	1
0	1	1	1	1	1
1	0	1	0	0	0
1	1	1	1	1	1

In jeder Zeile der Wahrheitstafel, in der in der mit „ $\varphi$ “ beschrifteten Spalte eine 1 steht, steht auch in der mit „ $\psi$ “ beschrifteten Spalte eine 1. Somit gilt  $\varphi \models \psi$ .

Andererseits steht in Zeile 1 in der mit „ $\psi$ “ beschrifteten Spalte eine 1 und in der mit „ $\varphi$ “ beschrifteten Spalte eine 0. Für die entsprechende Interpretation  $\mathcal{I}$  (mit  $\mathcal{I}(X) = 0$  und  $\mathcal{I}(Y) = 0$ ) gilt also  $\llbracket \psi \rrbracket^{\mathcal{I}} = 1$  und  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 0$ . Daher gilt  $\psi \not\models \varphi$ .

Folie 74

**Beispiel 2.17.** Für alle Formeln  $\varphi, \psi \in \text{AL}$  gilt:

$$\{\varphi, (\varphi \rightarrow \psi)\} \models \psi.$$

Dies folgt unmittelbar aus der Definition der Semantik:

Sei  $\mathcal{I}$  eine Interpretation mit  $\mathcal{I} \models \{\varphi, (\varphi \rightarrow \psi)\}$ . Dann gilt:

(1)  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 1$  und

(2)  $\llbracket (\varphi \rightarrow \psi) \rrbracket^{\mathcal{I}} = 1$ , d.h. es gilt  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 0$  oder  $\llbracket \psi \rrbracket^{\mathcal{I}} = 1$ .

Da  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 1$  gemäß (1) gilt, folgt gemäß (2), dass  $\llbracket \psi \rrbracket^{\mathcal{I}} = 1$ .

**Bemerkung.** Man kann die Folgerungsbeziehung  $\{\varphi, (\varphi \rightarrow \psi)\} \models \psi$  als eine formale Schlussregel auffassen (ähnlich den Syllogismen in Kapitel 1): Wenn  $\varphi$  und  $(\varphi \rightarrow \psi)$  gelten, so muss auch  $\psi$  gelten.

Diese Regel, die unter dem Namen *Modus Ponens* bekannt ist, ist von grundlegender Bedeutung in der Logik.

Folie 75

## Zusammenhänge

**Lemma 2.18** (Allgemeingültigkeit, Unerfüllbarkeit und Folgerung).

Für jede Formel  $\varphi \in \text{AL}$  gilt:

(a)  $\varphi$  ist allgemeingültig  $\iff \neg\varphi$  ist unerfüllbar  $\iff \mathbf{1} \models \varphi$ .

(b)  $\varphi$  ist unerfüllbar  $\iff \varphi \models \mathbf{0}$ .

*Beweis.*

(a) Zur Erinnerung: Wir schreiben kurz „ $\models \varphi$ “ um auszudrücken, dass die Formel  $\varphi$  allgemeingültig ist. Es gilt:

$$\begin{aligned} \models \varphi &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \not\models \neg\varphi \\ &\iff \neg\varphi \text{ ist unerfüllbar.} \end{aligned}$$

Außerdem gilt:

$$\begin{aligned} \mathbf{1} \models \varphi &\iff \text{für alle Interpretationen } \mathcal{I} \text{ mit } \mathcal{I} \models \mathbf{1} \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \varphi \text{ ist allgemeingültig.} \end{aligned}$$

(b) Es gilt:

$$\begin{aligned} &\varphi \text{ ist unerfüllbar} \\ \iff &\text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \not\models \varphi \\ \iff &\text{für alle Interpretationen } \mathcal{I} \text{ mit } \mathcal{I} \models \varphi \text{ gilt: } \mathcal{I} \models \mathbf{0} \\ \iff &\varphi \models \mathbf{0}. \end{aligned}$$

□

Folie 76

**Lemma 2.19** (Erfüllbarkeit und die Folgerungsbeziehung).  
Für alle Formelmengen  $\Phi \subseteq \text{AL}$  und für alle Formeln  $\psi \in \text{AL}$  gilt:

$$\Phi \models \psi \iff \Phi \cup \{\neg\psi\} \text{ ist unerfüllbar.}$$

*Beweis.*

„ $\implies$ “: Es gelte  $\Phi \models \psi$ . Sei  $\mathcal{I}$  eine beliebige Interpretation. Unser Ziel ist, zu zeigen, dass  $\mathcal{I} \not\models \Phi \cup \{\neg\psi\}$ .

*Fall 1:*  $\mathcal{I} \not\models \Phi$ .

Dann gilt insbesondere, dass  $\mathcal{I} \not\models \Phi \cup \{\neg\psi\}$ .

*Fall 2:*  $\mathcal{I} \models \Phi$ .

Wegen  $\Phi \models \psi$  gilt dann  $\mathcal{I} \models \psi$ .

Somit gilt:  $\mathcal{I} \not\models \neg\psi$ , und daher auch  $\mathcal{I} \not\models \Phi \cup \{\neg\psi\}$ .

Damit gilt in jedem Fall, dass  $\mathcal{I} \not\models \Phi \cup \{\neg\psi\}$ . Weil  $\mathcal{I}$  beliebig gewählt war, bedeutet dies, dass  $\Phi \cup \{\neg\psi\}$  unerfüllbar ist.

„ $\Leftarrow$ “: Sei  $\Phi \cup \{\neg\psi\}$  unerfüllbar. Unser Ziel ist, zu zeigen, dass  $\Phi \models \psi$ .

Dazu sei  $\mathcal{I}$  eine beliebige Interpretation mit  $\mathcal{I} \models \Phi$ . Wir müssen zeigen, dass  $\mathcal{I} \models \psi$ .

Da  $\Phi \cup \{\neg\psi\}$  unerfüllbar ist, muss gelten:  $\mathcal{I} \not\models \neg\psi$  (denn sonst würde  $\mathcal{I} \models \Phi \cup \{\neg\psi\}$  gelten). Somit gilt  $\mathcal{I} \models \psi$ .

□

Folie 77

**Lemma 2.20** (Allgemeingültigkeit und die Folgerungsbeziehung).

(a) Für jede Formel  $\varphi \in \text{AL}$  gilt:

$\varphi$  ist allgemeingültig  $\iff \varphi$  folgt aus der leeren Menge,

kurz:

$$\models \varphi \iff \emptyset \models \varphi.$$

(b) Für jede Formel  $\psi \in \text{AL}$  und jede endliche Formelmenge

$\Phi = \{\varphi_1, \dots, \varphi_n\} \subseteq \text{AL}$  gilt:

$\Phi \models \psi \iff (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$  ist allgemeingültig.

*Beweis.*

(a) Man beachte, dass für alle Interpretationen  $\mathcal{I}$  und für alle Formeln  $\psi \in \emptyset$  gilt:  $\mathcal{I} \models \psi$ . Daher gilt  $\mathcal{I} \models \emptyset$  für alle Interpretationen  $\mathcal{I}$ . Somit erhalten wir:

$$\begin{aligned} \emptyset \models \varphi &\iff \text{für alle Interpretationen } \mathcal{I} \text{ mit } \mathcal{I} \models \emptyset \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \varphi \text{ ist allgemeingültig, d.h. } \models \varphi. \end{aligned}$$

(b) „ $\implies$ “: Es gelte  $\Phi \models \psi$ . Sei  $\mathcal{I}$  eine beliebige Interpretation. Unser Ziel ist, zu zeigen, dass gilt:  $\mathcal{I} \models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$ .

*Fall 1:*  $\mathcal{I} \models \Phi$ , d.h.  $\mathcal{I} \models (\varphi_1 \wedge \dots \wedge \varphi_n)$ .

Wegen  $\Phi \models \psi$  gilt dann auch:  $\mathcal{I} \models \psi$ .

Somit gilt auch:  $\mathcal{I} \models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$ .

*Fall 2:*  $\mathcal{I} \not\models \Phi$ .

Dann gibt es ein  $i \in [n]$ , so dass  $\mathcal{I} \not\models \varphi_i$ .

Insbesondere gilt daher:  $\mathcal{I} \not\models (\varphi_1 \wedge \dots \wedge \varphi_n)$ .

Also gilt:  $\mathcal{I} \models (\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$ .

„ $\Leftarrow$ “: Sei die Formel  $(\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$  allgemeingültig. Wir wollen zeigen, dass  $\Phi \models \psi$  gilt.

Dazu sei  $\mathcal{I}$  eine beliebige Interpretation mit  $\mathcal{I} \models \Phi$ . Ziel ist, zu zeigen, dass  $\mathcal{I} \models \psi$ .

Wegen  $\mathcal{I} \models \Phi$  gilt:  $\mathcal{I} \models (\varphi_1 \wedge \dots \wedge \varphi_n)$ . Da die Formel  $(\varphi_1 \wedge \dots \wedge \varphi_n) \rightarrow \psi$  allgemeingültig ist, muss daher auch gelten:  $\mathcal{I} \models \psi$ .

□

Folie 78

### **Bemerkung 2.21.**

Aus den beiden vorigen Lemmas erhält man leicht, dass für alle Formeln  $\varphi, \psi \in \text{AL}$  gilt:

$$\varphi \models \psi \iff (\varphi \rightarrow \psi) \text{ ist allgemeingültig} \iff (\varphi \wedge \neg\psi) \text{ ist unerfüllbar.}$$

*Beweis.* Es sei  $\Phi := \{\varphi\}$ . Gemäß Lemma 2.20 gilt:

$$\Phi \models \psi \iff (\varphi \rightarrow \psi) \text{ ist allgemeingültig.}$$

Somit gilt:  $\varphi \models \psi \iff (\varphi \rightarrow \psi)$  ist allgemeingültig.

Außerdem gilt gemäß Lemma 2.19:

$$\Phi \models \psi \iff \Phi \cup \{\neg\psi\} \text{ ist unerfüllbar.}$$

Somit gilt:  $\varphi \models \psi \iff (\varphi \wedge \neg\psi)$  ist unerfüllbar.

□

## 2.2 Aussagenlogische Modellierung

### Beispiel 1: Sudoku

Folie 79

#### Sudoku

	3							
			1	9	5			
	9	8					6	
8				6				
4					3			1
				2				
	6					2	8	
			4	1	9			5
							7	

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Folie 80

#### Aussagenlogisches Modell

##### Koordinaten der Felder:

Feld  $(i, j)$  ist das Feld in Zeile  $i$  und Spalte  $j$ .

##### Aussagensymbole:

Aussagensymbol  $P_{i,j,k}$ , für  $i, j, k \in [9]$ , steht für die Aussage

„Das Feld mit den Koordinaten  $(i, j)$  enthält die Zahl  $k$ .“

Interpretationen beschreiben also Beschriftungen des  $9 \times 9$ -Gitters.

##### Ziel:

Für jede Anfangsbeschriftung  $A$  eine Formelmenge  $\Phi_A$ , so dass für alle Interpretationen  $\mathcal{I}$  gilt:

$$\mathcal{I} \models \Phi_A \iff \mathcal{I} \text{ beschreibt eine korrekte Lösung.}$$

Folie 81

Wir beschreiben zunächst eine Formelmenge  $\Phi = \{\varphi_1, \dots, \varphi_5\}$ , die die Grundregeln des Spiels beschreibt.

**Beschriftungen:**

„Auf jedem Feld steht mindestens eine Zahl“:

$$\varphi_1 := \bigwedge_{i,j=1}^9 \bigvee_{k=1}^9 P_{i,j,k}.$$

„Auf jedem Feld steht höchstens eine Zahl“:

$$\varphi_2 := \bigwedge_{i,j=1}^9 \bigwedge_{\substack{k,\ell=1 \\ k \neq \ell}}^9 \neg(P_{i,j,k} \wedge P_{i,j,\ell}).$$

Folie 82

**Zeilen:**

„Jede Zahl kommt in jeder Zeile vor“:

$$\varphi_3 := \bigwedge_{i=1}^9 \bigwedge_{k=1}^9 \bigvee_{j=1}^9 P_{i,j,k}.$$

**Spalten:**

„Jede Zahl kommt in jeder Spalte vor“:

$$\varphi_4 := \bigwedge_{j=1}^9 \bigwedge_{k=1}^9 \bigvee_{i=1}^9 P_{i,j,k}.$$

**Blöcke:**

„Jede Zahl kommt in jedem Block vor“:

$$\varphi_5 := \bigwedge_{i,j=0}^2 \bigwedge_{k=1}^9 \bigvee_{i',j'=1}^3 P_{3i+i',3j+j',k}.$$

Folie 83

**Anfangsbeschriftung:**

Sei  $A$  die Anfangsbeschriftung. Wir setzen

$$\Phi_A := \Phi \cup \{ P_{i,j,k} : A \text{ beschriftet Feld } (i, j) \text{ mit der Zahl } k \}.$$



### Automatische Lösung von Sudokus:

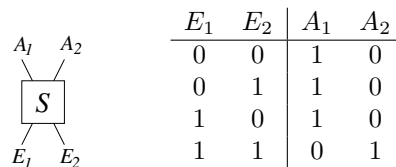
Um ein Sudoku mit Anfangsbeschriftung  $A$  zu lösen, können wir nun einfach die Formel  $\psi_A := \bigwedge_{\varphi \in \Phi_A} \varphi$  bilden und die Wahrheitstafel zu dieser Formel aufstellen. Falls die Wahrheitstafel zeigt, dass  $\psi_A$  kein Modell besitzt, so ist das Sudoku nicht lösbar. Andernfalls können wir ein beliebiges Modell  $\mathcal{I}$  von  $\psi_A$  hernehmen und daran die Lösung des Sudokus ablesen: Für jedes Feld  $(i, j)$  gibt es gemäß unserer Konstruktion der Formel  $\psi_A$  genau eine Zahl  $k \in [9]$ , so dass  $\mathcal{I}(P_{i,j,k}) = 1$  ist. Diese Zahl  $k$  können wir in Feld  $(i, j)$  eintragen und erhalten damit eine Lösung des Sudokus.

### Beispiel 2: Automatische Hardwareverifikation

#### Digitale Schaltkreise

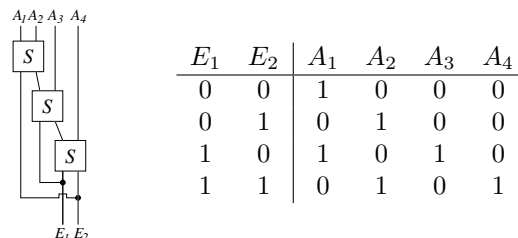
- Digitale *Signale* werden beschrieben durch 0 („aus“) und 1 („ein“).
- *Schaltelemente* berechnen ein oder mehrere Ausgangssignale aus einem oder mehreren Eingangssignalen. Das Ein-/Ausgabeverhalten eines Schaltelements lässt sich durch Wahrheitstafeln beschreiben.

*Beispiel:*



- *Schaltkreise* sind Kombinationen solcher Schaltelemente.

*Beispiel:*

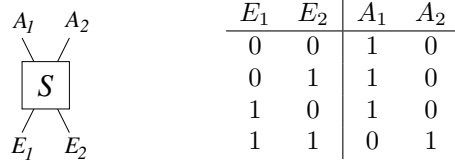


#### Formalisierung in der Aussagenlogik

*Schaltelement:*

- Für jeden Ein- und Ausgang ein Aussagensymbol.
- Für jeden Ausgang eine Formel, die den Wert der Ausgangs in Abhängigkeit von den Eingängen beschreibt.

Beispiel:



Aussagensymbole:

$P_1, P_2, Q_1, Q_2$

Formeln:

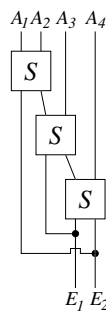
$Q_1 \leftrightarrow \neg(P_1 \wedge P_2)$

$Q_2 \leftrightarrow (P_1 \wedge P_2)$

Schaltkreis:

- Für jeden Ein- und Ausgang ein Aussagensymbol, sowie für jedes Schaltelement ein Sortiment von Aussagensymbolen.
- Formeln für die Schaltelemente und Formeln für die „Verdrahtung“.

Beispiel:



$E_1$	$E_2$	$A_1$	$A_2$	$A_3$	$A_4$
0	0	1	0	0	0
0	1	0	1	0	0
1	0	1	0	1	0
1	1	0	1	0	1

Aussagensymbole:

$P_1, P_2, Q_1, Q_2, Q_3, Q_4,$

$P_1^u, P_2^u, Q_1^u, Q_2^u,$

$P_1^m, P_2^m, Q_1^m, Q_2^m,$

$P_1^o, P_2^o, Q_1^o, Q_2^o.$

Formeln:

$Q_1^u \leftrightarrow \neg(P_1^u \wedge P_2^u),$

$Q_2^u \leftrightarrow (P_1^u \wedge P_2^u),$

$Q_1^m \leftrightarrow \neg(P_1^m \wedge P_2^m),$

$Q_2^m \leftrightarrow (P_1^m \wedge P_2^m),$

$Q_1^o \leftrightarrow \neg(P_1^o \wedge P_2^o),$

$Q_2^o \leftrightarrow (P_1^o \wedge P_2^o),$

$P_1^u \leftrightarrow P_1, P_2^u \leftrightarrow P_2,$

$P_1^m \leftrightarrow P_1, P_2^m \leftrightarrow Q_1^u,$

$P_1^o \leftrightarrow P_2, P_2^o \leftrightarrow Q_1^m,$

$Q_1 \leftrightarrow Q_1^o, Q_2 \leftrightarrow Q_2^o,$

$Q_3 \leftrightarrow Q_2^m, Q_4 \leftrightarrow Q_2^u.$

## Verifikation

### Ziel:

Nachweis, dass der Schaltkreis eine gewisse *Korrektheitsbedingung* erfüllt.

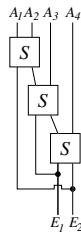
### Methode:

1. Beschreibe den Schaltkreis durch eine Menge  $\Phi$  von Formeln.
2. Formuliere die Korrektheitsbedingung als Formel  $\psi$ .
3. Weise nach, dass  $\psi$  aus  $\Phi$  folgt (bzw., dass  $\Phi \cup \{\neg\psi\}$  unerfüllbar ist).

**Bemerkung.** Bei Bedarf kann die Korrektheitsbedingung insbesondere so gewählt werden, dass sie das gewünschte Ein-/Ausgabeverhalten des Schaltkreises vollständig spezifiziert.

## Beispiele für Korrektheitsbedingungen

*Schaltkreis:*



*Einige Korrektheitsbedingungen:*

- Bei jeder Eingabe ist mindestens eine Ausgabe 1:

$$Q_1 \vee Q_2 \vee Q_3 \vee Q_4.$$

- Bei keiner Eingabe sind mehr als zwei Ausgaben 1:

$$\neg \bigvee_{1 \leq i < j < k \leq 4} (Q_i \wedge Q_j \wedge Q_k)$$

*Vollständige Spezifikation des Ein-/Ausgabeverhaltens:*

$$\begin{aligned} & \left( \neg P_1 \wedge \neg P_2 \rightarrow Q_1 \wedge \neg Q_2 \wedge \neg Q_3 \wedge \neg Q_4 \right) \\ \wedge & \left( \neg P_1 \wedge P_2 \rightarrow \neg Q_1 \wedge Q_2 \wedge \neg Q_3 \wedge \neg Q_4 \right) \\ \wedge & \left( P_1 \wedge \neg P_2 \rightarrow Q_1 \wedge \neg Q_2 \wedge Q_3 \wedge \neg Q_4 \right) \\ \wedge & \left( P_1 \wedge P_2 \rightarrow \neg Q_1 \wedge Q_2 \wedge \neg Q_3 \wedge Q_4 \right) \end{aligned}$$

## 2.3 Äquivalenz und Adäquatheit

Folie 84

### Äquivalenz

**Definition 2.22.** Zwei Formeln  $\varphi, \psi \in \text{AL}$  sind *äquivalent* (wir schreiben  $\varphi \equiv \psi$ ), wenn sie von den selben Interpretationen erfüllt werden, d.h., wenn für alle Interpretationen  $\mathcal{I}$  gilt:  $\mathcal{I} \models \varphi \iff \mathcal{I} \models \psi$ .

Zwei Formelmengen  $\Phi, \Psi \subseteq \text{AL}$  sind *äquivalent* (wir schreiben  $\Phi \equiv \Psi$ ), wenn sie von den selben Interpretationen erfüllt werden, d.h., wenn für alle Interpretationen  $\mathcal{I}$  gilt:  $\mathcal{I} \models \Phi \iff \mathcal{I} \models \Psi$ .

### Beobachtung 2.23.

- (a) Zwei Formeln  $\varphi, \psi \in \text{AL}$  sind genau dann äquivalent, wenn in den letzten Spalten ihrer Wahrheitstabellen jeweils die gleichen Einträge stehen.
- (b) Für endliche Formelmengen  $\Phi = \{\varphi_1, \dots, \varphi_m\}$ ,  $\Psi = \{\psi_1, \dots, \psi_n\} \subseteq \text{AL}$  gilt

$$\Phi \equiv \Psi \iff \bigwedge_{i=1}^m \varphi_i \equiv \bigwedge_{j=1}^n \psi_j.$$

*Beispiel:*

Für alle  $X, Y \in \text{AS}$  gilt:  $\neg(X \vee Y) \equiv (\neg X \wedge \neg Y)$  und  $X \equiv \neg\neg X$ .

Folie 85

### Äquivalenz und Allgemeingültigkeit

**Lemma 2.24.** (a) Für alle Formeln  $\varphi, \psi \in \text{AL}$  gilt:

$$\varphi \equiv \psi \iff (\varphi \leftrightarrow \psi) \text{ ist allgemeingültig.}$$

(b) Für alle  $\varphi \in \text{AL}$  gilt:

$$\varphi \text{ ist allgemeingültig} \iff \varphi \equiv \mathbf{1}.$$

*Beweis.*

(a)

$$\begin{aligned} \varphi \equiv \psi &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } (\mathcal{I} \models \varphi \iff \mathcal{I} \models \psi) \\ &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \models (\varphi \leftrightarrow \psi) \\ &\iff \models (\varphi \leftrightarrow \psi). \end{aligned}$$

(b)

$$\begin{aligned} \models \varphi &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } \mathcal{I} \models \varphi \\ &\iff \text{für alle Interpretationen } \mathcal{I} \text{ gilt: } (\mathcal{I} \models \varphi \iff \mathcal{I} \models \mathbf{1}) \\ &\iff \varphi \equiv \mathbf{1}. \end{aligned}$$

□

Folie 86

## Fundamentale Äquivalenzen

**Satz 2.25.** Für alle Formeln  $\varphi, \psi, \chi \in \text{AL}$  gelten die folgenden Äquivalenzen:

(a) *Idempotenz:*

$$(\varphi \wedge \varphi) \equiv \varphi, \quad (\varphi \vee \varphi) \equiv \varphi.$$

(b) *Kommutativität:*

$$(\varphi \wedge \psi) \equiv (\psi \wedge \varphi), \quad (\varphi \vee \psi) \equiv (\psi \vee \varphi).$$

(c) *Assoziativität:*

$$((\varphi \wedge \psi) \wedge \chi) \equiv (\varphi \wedge (\psi \wedge \chi)), \quad ((\varphi \vee \psi) \vee \chi) \equiv (\varphi \vee (\psi \vee \chi)).$$

(d) *Absorption:*

$$(\varphi \wedge (\varphi \vee \psi)) \equiv \varphi, \quad (\varphi \vee (\varphi \wedge \psi)) \equiv \varphi.$$

Folie 87

(e) *Distributivität:*

$$(\varphi \wedge (\psi \vee \chi)) \equiv ((\varphi \wedge \psi) \vee (\varphi \wedge \chi)), \quad (\varphi \vee (\psi \wedge \chi)) \equiv ((\varphi \vee \psi) \wedge (\varphi \vee \chi)).$$

(f) *Doppelte Negation:*

$$\neg\neg\varphi \equiv \varphi.$$

(g) *De Morgansche Regeln:*

$$\neg(\varphi \wedge \psi) \equiv (\neg\varphi \vee \neg\psi), \quad \neg(\varphi \vee \psi) \equiv (\neg\varphi \wedge \neg\psi).$$

(h) *Tertium Non Datur:*

$$(\varphi \wedge \neg\varphi) \equiv \mathbf{0}, \quad (\varphi \vee \neg\varphi) \equiv \mathbf{1}.$$

Folie 88

(i)

$$\begin{aligned} (\varphi \wedge \mathbf{1}) &\equiv \varphi, & (\varphi \vee \mathbf{0}) &\equiv \varphi, \\ (\varphi \wedge \mathbf{0}) &\equiv \mathbf{0}, & (\varphi \vee \mathbf{1}) &\equiv \mathbf{1}. \end{aligned}$$

(j)

$$\mathbf{1} \equiv \neg\mathbf{0}, \quad \mathbf{0} \equiv \neg\mathbf{1}.$$

(k) *Elimination der Implikation:*

$$(\varphi \rightarrow \psi) \equiv (\neg\varphi \vee \psi).$$

Folie 89

*Beweis.* Alle hier genannten Äquivalenzen können leicht mit Hilfe der Wahrheitstafelmethode überprüft werden.

Zum Beispiel die erste de Morgansche Regel:

$$\neg(\varphi \wedge \psi) \equiv (\neg\varphi \vee \neg\psi).$$

Wir berechnen dazu folgende Wahrheitstafeln:

$\varphi$	$\psi$	$(\varphi \wedge \psi)$	$\neg(\varphi \wedge \psi)$
0	0	0	1
0	1	0	1
1	0	0	1
1	1	1	0

$\varphi$	$\psi$	$\neg\varphi$	$\neg\psi$	$(\neg\varphi \vee \neg\psi)$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	1
1	1	0	0	0

Die letzten Spalten der beiden Wahrheitstafeln sind gleich, also sind die Formeln äquivalent.

*Rest:* Übung. □

**Bemerkung.** Durch schrittweises Anwenden der in Satz 2.25 aufgelisteten Äquivalenzen kann man eine gegebene Formel in eine zu ihr äquivalente Formel umformen.

## Das Dualitätsprinzip

**Definition 2.26.** Sei  $\varphi \in \text{AL}$  eine Formel, in der keine Implikationen vorkommt.

Die zu  $\varphi$  *duale Formel* ist die Formel  $\tilde{\varphi} \in \text{AL}$ , die aus  $\varphi$  entsteht, indem man überall  $\mathbf{0}$  durch  $\mathbf{1}$ ,  $\mathbf{1}$  durch  $\mathbf{0}$ ,  $\wedge$  durch  $\vee$  und  $\vee$  durch  $\wedge$  ersetzt.

*Beispiel.* Für  $\varphi := ((A_1 \wedge \mathbf{0}) \vee \neg(A_2 \vee \mathbf{1}))$  ist  $\tilde{\varphi} = ((A_1 \vee \mathbf{1}) \wedge \neg(A_2 \wedge \mathbf{0}))$ .

**Satz 2.27** (Dualitätssatz der Aussagenlogik).

Für alle Formeln  $\varphi, \psi \in \text{AL}$ , in denen keine Implikation vorkommt, gilt:

$$\varphi \equiv \psi \quad \iff \quad \tilde{\varphi} \equiv \tilde{\psi}.$$

Wir werden den Dualitätssatz per Induktion über den Aufbau von Formeln beweisen.

## Beweise per Induktion über den Aufbau von Formeln

- Ähnlich wie wir Aussagen über die natürlichen Zahlen durch vollständige Induktion beweisen können, können wir Aussagen über Formeln per *Induktion über den Aufbau der Formeln* beweisen.
- Im *Induktionsanfang* beweisen wir die Aussagen für die atomaren Formeln, und im *Induktionsschritt* schließen wir von den Bestandteilen einer Formel auf die Formel selbst.
- Dieses Vorgehen ist z.B. dadurch gerechtfertigt, dass es sich auch als vollständige Induktion über die Höhe des Syntaxbaumes auffassen lässt.

Folie 93

Schematisch sieht der Beweis einer Aussage  $\mathbb{A}(\varphi)$  für alle Formeln  $\varphi \in \text{AL}$  wie folgt aus:

*Induktionsanfang:*

- Beweise  $\mathbb{A}(\mathbf{0})$  und  $\mathbb{A}(\mathbf{1})$ .
- Beweise  $\mathbb{A}(X)$  für alle  $X \in \text{AS}$ .

*Induktionsschritt:*

- Beweise  $\mathbb{A}(\neg\varphi)$  unter der Annahme, dass  $\mathbb{A}(\varphi)$  gilt.
- Beweise  $\mathbb{A}((\varphi \wedge \psi))$  unter der Annahme, dass  $\mathbb{A}(\varphi)$  und  $\mathbb{A}(\psi)$  gelten.
- Beweise  $\mathbb{A}((\varphi \vee \psi))$  unter der Annahme, dass  $\mathbb{A}(\varphi)$  und  $\mathbb{A}(\psi)$  gelten.
- Beweise  $\mathbb{A}((\varphi \rightarrow \psi))$  unter der Annahme, dass  $\mathbb{A}(\varphi)$  und  $\mathbb{A}(\psi)$  gelten.

Folie 94

Um den Dualitätssatz zu beweisen benötigen wir zunächst noch eine Definition. Der Kern des Beweises steckt im darauf folgenden Lemma.

**Definition 2.28.** Sei  $\mathcal{I}$  eine Interpretation. Die zu  $\mathcal{I}$  *duale Interpretation*  $\tilde{\mathcal{I}}$  ist definiert durch  $\tilde{\mathcal{I}}(X) := 1 - \mathcal{I}(X)$  für alle  $X \in \text{AS}$ .

D.h. für alle Aussagensymbole  $X$  gilt:

$$\tilde{\mathcal{I}}(X) = \begin{cases} 0, & \text{falls } \mathcal{I}(X) = 1 \\ 1, & \text{falls } \mathcal{I}(X) = 0 \end{cases}$$

**Lemma 2.29.** Für alle Formeln  $\varphi \in \text{AL}$ , in denen keine Implikation vorkommt, und alle Interpretationen  $\mathcal{I}$  gilt:

$$\mathcal{I} \models \tilde{\varphi} \iff \tilde{\mathcal{I}} \not\models \varphi.$$

*Beweis von Lemma 2.29.*

Sei  $\mathcal{I}$  eine beliebige Interpretation.

Per Induktion über den Aufbau von Formeln zeigen wir, dass für jedes  $\varphi \in \text{AL}$ , in dem keine Implikation vorkommt gilt:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}.$$

*Beachte:* Dann gilt natürlich auch:  $\mathcal{I} \models \tilde{\varphi} \iff \tilde{\mathcal{I}} \not\models \varphi$ .

*Induktionsanfang:*



- Sei  $\varphi := \mathbf{1}$ . Dann ist  $\tilde{\varphi} = \mathbf{0}$ . Zu zeigen:  $\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$ . Beweis:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = \llbracket \mathbf{0} \rrbracket^{\mathcal{I}} = 0 = 1 - 1 = 1 - \llbracket \mathbf{1} \rrbracket^{\tilde{\mathcal{I}}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}.$$

- Sei  $\varphi := \mathbf{0}$ . Dann ist  $\tilde{\varphi} = \mathbf{1}$ . Zu zeigen:  $\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$ . Beweis:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = \llbracket \mathbf{1} \rrbracket^{\mathcal{I}} = 1 = 1 - 0 = 1 - \llbracket \mathbf{0} \rrbracket^{\tilde{\mathcal{I}}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}.$$

- Sei  $\varphi := X$  für ein  $X \in \text{AS}$ . Dann ist  $\tilde{X} = X$ .

Zu zeigen:  $\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$ . Beweis:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = \llbracket X \rrbracket^{\mathcal{I}} = \mathcal{I}(X) = 1 - \tilde{\mathcal{I}}(X) = 1 - \llbracket X \rrbracket^{\tilde{\mathcal{I}}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}.$$

*Induktionsschritt:*

- *Negation:*

Gemäß Induktionsannahme gilt:  $\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$ .

Wir wollen zeigen, dass auch gilt:  $\llbracket \widetilde{\neg\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \neg\varphi \rrbracket^{\tilde{\mathcal{I}}}$ .

Per Definition ist  $\widetilde{\neg\varphi} = \neg\tilde{\varphi}$ . Damit gilt:

$$\llbracket \widetilde{\neg\varphi} \rrbracket^{\mathcal{I}} = \llbracket \neg\tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} \stackrel{(\text{IA})}{=} 1 - (1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}) = 1 - \llbracket \neg\varphi \rrbracket^{\tilde{\mathcal{I}}}.$$

- *Konjunktion:*

Gemäß Induktionsannahme gilt:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}} \quad \text{und} \quad \llbracket \tilde{\psi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \psi \rrbracket^{\tilde{\mathcal{I}}}.$$

Wir wollen zeigen, dass auch gilt:  $\llbracket \widetilde{(\varphi \wedge \psi)} \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \wedge \psi) \rrbracket^{\tilde{\mathcal{I}}}$ .

Per Definition ist  $\widetilde{(\varphi \wedge \psi)} = (\tilde{\varphi} \vee \tilde{\psi})$ .

Folgende Wahrheitstafel, bei der die 4. und 5. Spalte auf der Induktionsannahme beruht, zeigt, dass  $\llbracket (\tilde{\varphi} \vee \tilde{\psi}) \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \wedge \psi) \rrbracket^{\tilde{\mathcal{I}}}$ .

$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}}$	$\llbracket \tilde{\psi} \rrbracket^{\mathcal{I}}$	$\llbracket (\tilde{\varphi} \vee \tilde{\psi}) \rrbracket^{\mathcal{I}}$	$\llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$	$\llbracket \psi \rrbracket^{\tilde{\mathcal{I}}}$	$\llbracket (\varphi \wedge \psi) \rrbracket^{\tilde{\mathcal{I}}}$
0	0	0	1	1	1
0	1	1	1	0	0
1	0	1	0	1	0
1	1	1	0	0	0

Die 3. und 6. Spalte zeigt, dass  $\llbracket (\tilde{\varphi} \vee \tilde{\psi}) \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \wedge \psi) \rrbracket^{\tilde{\mathcal{I}}}$  gilt.

- *Disjunktion:*

Gemäß Induktionsannahme gilt:

$$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}} \quad \text{und} \quad \llbracket \tilde{\psi} \rrbracket^{\mathcal{I}} = 1 - \llbracket \psi \rrbracket^{\tilde{\mathcal{I}}}.$$

Wir wollen zeigen, dass auch gilt:  $\llbracket \widetilde{(\varphi \vee \psi)} \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \vee \psi) \rrbracket^{\tilde{\mathcal{I}}}$ .

Per Definition ist  $\widetilde{(\varphi \vee \psi)} = (\tilde{\varphi} \wedge \tilde{\psi})$ . Folgende Wahrheitstafel, bei der die 4. und 5. Spalte auf der Induktionsannahme beruht, zeigt, dass  $\llbracket (\tilde{\varphi} \wedge \tilde{\psi}) \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \vee \psi) \rrbracket^{\tilde{\mathcal{I}}}$ .

$\llbracket \tilde{\varphi} \rrbracket^{\mathcal{I}}$	$\llbracket \tilde{\psi} \rrbracket^{\mathcal{I}}$	$\llbracket (\tilde{\varphi} \wedge \tilde{\psi}) \rrbracket^{\mathcal{I}}$	$\llbracket \varphi \rrbracket^{\tilde{\mathcal{I}}}$	$\llbracket \psi \rrbracket^{\tilde{\mathcal{I}}}$	$\llbracket (\varphi \vee \psi) \rrbracket^{\tilde{\mathcal{I}}}$
0	0	0	1	1	1
0	1	0	1	0	1
1	0	0	0	1	1
1	1	1	0	0	0

Die 3. und 6. Spalte zeigt, dass  $\llbracket (\tilde{\varphi} \wedge \tilde{\psi}) \rrbracket^{\mathcal{I}} = 1 - \llbracket (\varphi \vee \psi) \rrbracket^{\tilde{\mathcal{I}}}$  gilt.

- *Implikation:*

Hier ist nichts zu zeigen, weil das Lemma nur über Formeln ohne Implikation spricht. □

Folie 95

*Beweis von Satz 2.27.*

Seien  $\varphi, \psi \in \text{AL}$  Formeln, in denen keine Implikation vorkommt.

Wir wollen zeigen, dass gilt:  $\varphi \equiv \psi \iff \tilde{\varphi} \equiv \tilde{\psi}$ .

„ $\implies$ “: Es gilt:<sup>1</sup>

$$\begin{aligned} & \varphi \equiv \psi \\ \implies & \text{F.a. Interpretationen } \mathcal{I} \text{ gilt: } (\tilde{\mathcal{I}} \models \varphi \iff \tilde{\mathcal{I}} \models \psi) \\ \stackrel{\text{Lemma 2.29}}{\implies} & \text{F.a. Interpretationen } \mathcal{I} \text{ gilt: } (\mathcal{I} \not\models \tilde{\varphi} \iff \mathcal{I} \not\models \tilde{\psi}) \\ \implies & \text{F.a. Interpretationen } \mathcal{I} \text{ gilt: } (\mathcal{I} \models \tilde{\varphi} \iff \mathcal{I} \models \tilde{\psi}) \\ \implies & \tilde{\varphi} \equiv \tilde{\psi}. \end{aligned}$$

---

<sup>1</sup>Wir schreiben kurz „f.a.“ als Abkürzung für die Worte „für alle“

„ $\Leftarrow$ “: Es gilt:

$$\begin{aligned} \tilde{\varphi} \equiv \tilde{\psi} &\implies \tilde{\varphi} \equiv \tilde{\psi} && \text{(andere Beweisrichtung)} \\ &\implies \varphi \equiv \psi && \text{(weil } \tilde{\varphi} = \varphi \text{ und } \tilde{\psi} = \psi\text{)}. \end{aligned}$$

□

Folie 96

## Funktionale Vollständigkeit der Aussagenlogik

Im Folgenden bezeichnen wir als *Wahrheitstafel* eine Tabelle mit  $n+1$  Spalten und  $2^n$  Zeilen, die für jedes Tupel  $(b_1, \dots, b_n) \in \{0, 1\}^n$  genau eine Zeile enthält, deren erste  $n$  Einträge  $b_1, \dots, b_n$  sind.

**Satz 2.30** (Funktionale Vollständigkeit der Aussagenlogik).

*Zu jeder Wahrheitstafel gibt es eine Formel  $\varphi \in AL$  mit dieser Wahrheitstafel.*

Mathematisch präzise lässt sich dieser Satzes wie folgt formulieren:

*Für alle  $n \in \mathbb{N}$  gibt es zu jeder Funktion  $F : \{0, 1\}^n \rightarrow \{0, 1\}$  eine Formel  $\varphi(A_1, \dots, A_n) \in AL$ , so dass für alle  $(b_1, \dots, b_n) \in \{0, 1\}^n$  gilt:*

$$F(b_1, \dots, b_n) = 1 \iff \varphi[b_1, \dots, b_n] = 1.$$

**Definition 2.31.** Funktionen  $F : \{0, 1\}^n \rightarrow \{0, 1\}$  (mit  $n \in \mathbb{N}$ ) nennt man *Boolesche Funktionen* (der Stelligkeit  $n$ ).

Bevor wir Satz 2.30 beweisen, betrachten wir zunächst ein Beispiel.

Folie 97

**Beispiel 2.32.** Betrachte die Wahrheitstafel  $T$ :

$b_1$	$b_2$	$b_3$	$F(b_1, b_2, b_3)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Eine Formel  $\varphi(A_1, A_2, A_3)$ , so dass  $T$  die Wahrheitstafel für  $\varphi$  ist, kann man folgendermaßen erzeugen:

- Betrachte alle Zeilen von  $T$ , bei denen in der letzten Spalte eine „1“ steht.
- Für jede solche Zeile konstruiere eine Formel, die genau von der zu der Zeile gehörenden Belegung von  $b_1, b_2, b_3$  erfüllt wird.
- Bilde die Disjunktion (d.h. die „Veroderung“) über all diese Formeln. Dies liefert die gesuchte Formel  $\varphi$ .

Folie 98

In unserer Beispiel-Wahrheitstafel  $T$  gibt es genau 3 Zeilen, bei denen in der letzten Spalte eine „1“ steht, nämlich die Zeilen

$b_1$	$b_2$	$b_3$	$F(b_1, b_2, b_3)$	zur jeweiligen Zeile gehörende Formel:
0	0	0	1	$(\neg A_1 \wedge \neg A_2 \wedge \neg A_3)$
0	0	1	1	$(\neg A_1 \wedge \neg A_2 \wedge A_3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
1	0	1	1	$(A_1 \wedge \neg A_2 \wedge A_3)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Insgesamt erhalten wir dadurch die zur Wahrheitstafel  $T$  passende Formel

$$\varphi = (\neg A_1 \wedge \neg A_2 \wedge \neg A_3) \vee (\neg A_1 \wedge \neg A_2 \wedge A_3) \vee (A_1 \wedge \neg A_2 \wedge A_3).$$

*Beweis von Satz 2.30.*

Sei  $F : \{0, 1\}^n \rightarrow \{0, 1\}$ . Falls  $F(\bar{b}) = 0$  für alle  $\bar{b} \in \{0, 1\}^n$ , so setzen wir  $\varphi(A_1, \dots, A_n) := \mathbf{0}$ .

Im Folgenden betrachten wir also nur noch den Fall, dass es mindestens ein  $\bar{b} \in \{0, 1\}^n$  mit  $F(\bar{b}) = 1$  gibt.

Für jedes  $i \in [n]$  sei

$$\lambda_{i,1} := A_i \quad \text{und} \quad \lambda_{i,0} := \neg A_i.$$

Für  $\bar{b} = (b_1, \dots, b_n) \in \{0, 1\}^n$  sei

$$\psi_{\bar{b}} := (\lambda_{1,b_1} \wedge \dots \wedge \lambda_{n,b_n})$$

*Beispiel:* Für  $n = 3$  und  $\bar{b} = (0, 1, 0)$  ist  $\psi_{(0,1,0)} = (\neg A_1 \wedge A_2 \wedge \neg A_3)$ .

Dann gilt für alle  $\bar{c} = (c_1, \dots, c_n) \in \{0, 1\}^n$ :

$$\psi_{\bar{b}}[\bar{c}] = 1 \iff \bar{b} = \bar{c}.$$

Nun sei

$$\varphi := \bigvee_{\substack{\bar{b} \in \{0,1\}^n \\ \text{mit } F(\bar{b})=1}} \psi_{\bar{b}}.$$

Dann gilt für alle  $\bar{c} \in \{0,1\}^n$ :

$$\varphi[\bar{c}] = 1$$

$$\iff \text{Es gibt ein } \bar{b} \in \{0,1\}^n \text{ mit } F(\bar{b}) = 1 \text{ und } \psi_{\bar{b}}[\bar{c}] = 1$$

$$\iff \text{Es gibt ein } \bar{b} \in \{0,1\}^n \text{ mit } F(\bar{b}) = 1 \text{ und } \bar{b} = \bar{c}$$

$$\iff F(\bar{c}) = 1.$$

□

Folie 99

## Adäquatheit

Satz 2.30 besagt, dass die Aussagenlogik AL die größtmögliche Ausdrucksstärke hat. Dafür reichen allerdings schon „kleinere“ Logiken, wie wir im Folgenden sehen werden.

**Definition 2.33.** Sei  $\tau \subseteq \{0, 1, \neg, \wedge, \vee, \rightarrow\}$ .

- (a)  $AL(\tau)$  sei das Fragment der Logik AL, das aus den Formeln besteht, in denen nur Junktoren und Konstanten aus  $\tau$  vorkommen.
- (b)  $\tau$  heißt *adäquat*, wenn jede Formel  $\varphi \in AL$  äquivalent zu einer Formel in  $AL(\tau)$  ist.

## Beispiele 2.34.

- (a)  $\{\neg, \wedge\}$ ,  $\{\neg, \vee\}$ ,  $\{0, \rightarrow\}$  sind adäquat.
- (b)  $\{\wedge, \vee, \rightarrow\}$  ist nicht adäquat.

*Beweis.*

- (a) Die Adäquatheit von  $\{\neg, \wedge\}$  folgt leicht aus Satz 2.25 (h) (Tertium Non Datur), (f) (doppelte Negation), (g) (De Morgan) und (k) (Elimination der Implikation):

- $\mathbf{0} \equiv (X \wedge \neg X)$ , für jedes  $X \in \text{AS}$
- $\mathbf{1} \equiv (X \vee \neg X)$ , für jedes  $X \in \text{AS}$
- für alle Formeln  $\varphi, \psi$  gilt:
  - $(\varphi \vee \psi) \equiv \neg(\neg\varphi \wedge \neg\psi)$
  - $(\varphi \rightarrow \psi) \equiv (\neg\varphi \vee \psi)$ .

Die Adäquatheit von  $\{\neg, \vee\}$  folgt aus der Adäquatheit von  $\{\neg, \wedge\}$  und der Tatsache, dass für alle Formeln  $\varphi, \psi$  gilt:

$$(\varphi \wedge \psi) \equiv \neg(\neg\varphi \vee \neg\psi).$$

Die Adäquatheit von  $\{\mathbf{0}, \rightarrow\}$  folgt aus der Adäquatheit von  $\{\neg, \vee\}$  und der Beobachtung, dass für alle Formeln  $\varphi, \psi$  gilt:

$$\neg\varphi \equiv (\varphi \rightarrow \mathbf{0}) \quad \text{und} \quad (\varphi \vee \psi) \equiv (\neg\varphi \rightarrow \psi).$$

Details: Übung.

- (b)  $\{\wedge, \vee, \rightarrow\}$  ist *nicht* adäquat, weil für alle Formeln  $\varphi(X_1, \dots, X_n) \in \text{AL}(\{\wedge, \vee, \rightarrow\})$  gilt:  $\varphi[1, \dots, 1] = 1$  (dies kann man per Induktion nach dem Formelaufbau leicht nachweisen; Details: Übung).

□

Folie 100

## Andere Junktoren

- Die Auswahl der Junktoren  $\neg, \wedge, \vee, \rightarrow$  (und  $\leftrightarrow$  als Abkürzung) für „unsere“ aussagenlogische Sprache richtet sich nach dem umgangssprachlichen Gebrauch und den Erfordernissen des formalen Schließens, ist aber in gewisser Weise willkürlich.
- Durch Festlegung ihrer Wahrheitstafeln können wir auch andere Junktoren definieren und erhalten daraus andere aussagenlogische Sprachen.
- Für jede Menge  $\tau$  von so definierten Junktoren und den booleschen Konstanten (die wir als „nullstellige“ Junktoren auffassen können) sei  $\text{AL}(\tau)$  die daraus gebildete aussagenlogische Sprache.
- Satz 2.30 besagt dann, dass jede Formel in  $\text{AL}(\tau)$  zu einer Formel in  $\text{AL}$  äquivalent ist. Gilt die Umkehrung ebenfalls, so bezeichnen wir  $\tau$  als *adäquat*.

Folie 101

## Beispiele 1: Exklusives Oder

Der 2-stellige Junktor  $\oplus$  sei definiert durch

$\varphi$	$\psi$	$(\varphi \oplus \psi)$
0	0	0
0	1	1
1	0	1
1	1	0

Intuitiv bedeutet  $(\varphi \oplus \psi)$  „entweder  $\varphi$  oder  $\psi$ “.  
 Man nennt  $\oplus$  auch *exklusives Oder*.

Folie 102

## Der dreistellige Mehrheitsjunktor

Der 3-stellige Junktor  $M$  sei definiert durch

$\varphi$	$\psi$	$\chi$	$M(\varphi, \psi, \chi)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Intuitiv ist  $M(\varphi, \psi, \chi)$  also genau dann wahr, wenn mindestens zwei (also die Mehrheit) der Formeln  $\varphi, \psi, \chi$  wahr sind.

Folie 103

## NAND

Der folgende zweistellige Junktor ist bekannt als *NAND-Gatter* (not-and) oder *Sheffer-Strich*:

$\varphi$	$\psi$	$(\varphi   \psi)$
0	0	1
0	1	1
1	0	1
1	1	0

**Satz 2.35.**  $\{|\}$  ist adäquat.

*Beweis.* Man kann sich leicht davon überzeugen, dass für alle Formeln  $\varphi, \psi$  gilt:

$$\neg\varphi \equiv (\varphi|\varphi) \quad \text{und} \quad (\varphi \wedge \psi) \equiv \neg(\varphi|\psi)$$

Details: Übung. □

## 2.4 Normalformen

Folie 104

### Vereinfachende Annahme

In diesem Abschnitt betrachten wir nur Formeln in  $\text{AL}(\{\neg, \vee, \wedge\})$ .

### Rechtfertigung

Die Annahme bedeutet keine wesentliche Einschränkung, weil die Menge  $\{\neg, \vee, \wedge\}$  adäquat ist.

Folie 105

### NNF

**Definition 2.36.** Eine Formel ist in *Negationsnormalform (NNF)*, wenn sie zu  $\text{AL}(\{\neg, \wedge, \vee\})$  gehört und Negationszeichen nur unmittelbar vor Aussagensymbolen auftreten.

**Satz 2.37.** Jede aussagenlogische Formel ist äquivalent zu einer Formel in NNF.

*Beweis.* Da  $\text{AL}(\{\neg, \wedge, \vee\})$  adäquat ist, genügt es, an Stelle von  $\text{AL}$  nur  $\text{AL}(\{\neg, \wedge, \vee\})$  zu betrachten.

Per Induktion über den Aufbau definieren wir zu jedem  $\varphi \in \text{AL}(\{\neg, \wedge, \vee\})$  zwei Formeln  $\varphi'$  und  $\varphi''$  in NNF, so dass gilt:

$$\varphi \equiv \varphi' \quad \text{und} \quad \neg\varphi \equiv \varphi''. \quad (\star)$$

*Induktionsanfang:*



Falls  $\varphi = X$  für ein  $X \in \text{AS}$ : Setze  $\varphi' := X$  und  $\varphi'' := \neg X$ .

Dann gilt  $(\star)$  offensichtlich.

*Induktionsschritt:*

Falls  $\varphi = \neg\psi$  für eine Formel  $\psi$ : Setze  $\varphi' := \psi''$  und  $\varphi'' := \psi'$ .

Dann folgt  $(\star)$  unmittelbar aus der Induktionsannahme.

Falls  $\varphi = (\psi_1 \wedge \psi_2)$  für Formeln  $\psi_1, \psi_2$ :

Setze  $\varphi' := (\psi'_1 \wedge \psi'_2)$  und  $\varphi'' := (\psi''_1 \vee \psi''_2)$ .

Gemäß Induktionsannahme gilt  $\psi_1 \equiv \psi'_1$  und  $\psi_2 \equiv \psi'_2$ , und daher gilt auch  $\varphi \equiv \varphi'$ .

Außerdem gilt gemäß Induktionsannahme, dass  $\neg\psi_1 \equiv \psi''_1$  und  $\neg\psi_2 \equiv \psi''_2$ . Daher gilt auch:

$$\begin{aligned} \neg\varphi &\equiv (\neg\psi_1 \vee \neg\psi_2) && \text{(De Morgan)} \\ &\equiv (\psi''_1 \vee \psi''_2) && \text{(Induktionsannahme)} \end{aligned}$$

Also gilt  $(\star)$ .

Falls  $\varphi = (\psi_1 \vee \psi_2)$  für Formeln  $\psi_1, \psi_2$ :

Setze  $\varphi' := (\psi'_1 \vee \psi'_2)$  und  $\varphi'' := (\psi''_1 \wedge \psi''_2)$ .

Ähnlich wie im Fall, dass  $\varphi = (\psi_1 \wedge \psi_2)$ , lässt sich zeigen, dass  $(\star)$  gilt.

Die Formeln  $\varphi'$  und  $\varphi''$  sind in NNF, weil Negationszeichen nur im Induktionsanfang verwendet werden und dort unmittelbar vor einem Aussagensymbol stehen. □

Folie 106

## Ein NNF-Algorithmus

**Eingabe:** Formel  $\varphi \in \text{AL}(\{\neg, \wedge, \vee\})$ .

**Ausgabe:** Formel  $\varphi'$  in NNF

**Verfahren:**

1. Wiederhole folgende Schritte:
2. Wenn  $\varphi$  in NNF ist, dann halte mit Ausgabe  $\varphi$ .

3. Ersetze eine Subformel von  $\varphi$  der Gestalt  
 $\neg(\psi_1 \wedge \psi_2)$  durch  $(\neg\psi_1 \vee \neg\psi_2)$   
oder eine Subformel der Gestalt  
 $\neg(\psi_1 \vee \psi_2)$  durch  $(\neg\psi_1 \wedge \neg\psi_2)$   
oder eine Subformel der Gestalt  
 $\neg\neg\psi$  durch  $\psi$ .  
Sei  $\varphi'$  die resultierende Formel.
4.  $\varphi := \varphi'$ .

Folie 107

### Korrektheit des NNF-Algorithmus

**Satz 2.38.** Für jede Eingabeformel  $\varphi \in \text{AL}(\{\neg, \wedge, \vee\})$  gibt der NNF-Algorithmus nach endlich vielen Schritten eine zu  $\varphi$  äquivalente Formel  $\varphi'$  in NNF aus.

(hier ohne Beweis)

**Bemerkung.** Unter Verwendung geeigneter Datenstrukturen lässt sich der NNF-Algorithmus mit linearer Laufzeit implementieren, d.h., Laufzeit  $O(n)$  bei Eingabe einer Formel der Länge  $n$ .

Folie 108

### Beispiel 2.39.

Das Ziel ist, die Formel  $\left(\left(\neg A_0 \wedge \neg((A_0 \vee A_1) \rightarrow A_0)\right) \rightarrow \mathbf{0}\right)$

in NNF zu bringen, d.h. eine zu ihr äquivalente Formel in NNF zu finden.

*Lösung:* Wir ersetzen zunächst die Konstanten  $\mathbf{0}$  und  $\mathbf{1}$  sowie alle Implikationspfeile durch geeignete Formeln aus  $\text{AL}(\{\neg, \wedge, \vee\})$  und wenden dann den NNF-Algorithmus an. Der Teil einer Formel, der als Nächstes

ersetzt wird, ist im Folgenden jeweils unterstrichen.

$$\begin{aligned}
 & \left( \left( \neg A_0 \wedge \neg((A_0 \vee A_1) \rightarrow A_0) \right) \rightarrow \underline{\mathbf{0}} \right) \\
 \equiv & \left( \left( \neg A_0 \wedge \neg((A_0 \vee A_1) \rightarrow A_0) \right) \underline{\Rightarrow} (A_0 \wedge \neg A_0) \right) \\
 \equiv & \left( \neg \left( \neg A_0 \wedge \neg((A_0 \vee A_1) \underline{\Rightarrow} A_0) \right) \vee (A_0 \wedge \neg A_0) \right) \\
 \equiv & \left( \underline{\neg} \left( \neg A_0 \wedge \neg(\neg(A_0 \vee A_1) \vee A_0) \right) \vee (A_0 \wedge \neg A_0) \right) \\
 \equiv & \left( \left( \underline{\neg} \neg A_0 \vee \underline{\neg} \neg(\neg(A_0 \vee A_1) \vee A_0) \right) \vee (A_0 \wedge \neg A_0) \right) \\
 \equiv & \left( \left( A_0 \vee (\underline{\neg}(A_0 \vee A_1) \vee A_0) \right) \vee (A_0 \wedge \neg A_0) \right) \\
 \equiv & \left( \left( A_0 \vee (\neg A_0 \wedge \neg A_1) \vee A_0 \right) \vee (A_0 \wedge \neg A_0) \right).
 \end{aligned}$$

Diese Formel ist offensichtlich in NNF.

Folie 109

### Klammern bei Konjunktionen und Disjunktionen

Weil  $\wedge$  assoziativ ist, können wir Formeln der Gestalt  $\bigwedge_{i=1}^n \varphi_i$  etwas großzügiger interpretieren. Von nun an stehe  $\bigwedge_{i=1}^n \varphi_i$  für  $\varphi_1 \wedge \dots \wedge \varphi_n$  mit *irgendeiner* Klammerung.

Entsprechend verfahren wir mit Disjunktionen.

*Beispiel.* Die Formel  $\bigwedge_{i=1}^4 \varphi_i$  kann für jede der folgenden Formeln stehen:

$$\begin{aligned}
 & (((\varphi_1 \wedge \varphi_2) \wedge \varphi_3) \wedge \varphi_4) , \\
 & ((\varphi_1 \wedge (\varphi_2 \wedge \varphi_3)) \wedge \varphi_4) , \\
 & ((\varphi_1 \wedge \varphi_2) \wedge (\varphi_3 \wedge \varphi_4)) , \\
 & (\varphi_1 \wedge ((\varphi_2 \wedge \varphi_3) \wedge \varphi_4)) , \\
 & (\varphi_1 \wedge (\varphi_2 \wedge (\varphi_3 \wedge \varphi_4))) .
 \end{aligned}$$

Folie 110

## DNF und KNF

### Definition 2.40.

- (a) Ein *Literal* ist eine Formel der Gestalt  $X$  oder  $\neg X$ , wobei  $X \in \text{AS}$ .  
 Im ersten Fall sprechen wir von einem *positiven*, im zweiten Fall von einem *negativen* Literal.

- (b) Eine Formel ist in *disjunktiver Normalform (DNF)*, wenn sie eine Disjunktion von Konjunktionen von Literalen ist, d.h., wenn sie die Form

$$\bigvee_{i=1}^n \left( \bigwedge_{j=1}^{m_i} \lambda_{i,j} \right)$$

hat, wobei  $n, m_1, \dots, m_n \geq 1$  sind und die  $\lambda_{i,j}$  für alle  $i \in [n]$  und  $j \in [m_i]$  Literale sind.

Die Subformeln  $\kappa_i := \bigwedge_{j=1}^{m_i} \lambda_{i,j}$ , für  $i \in [n]$ , nennen wir die (*konjunktiven*) *Klauseln* der Formel.

*Beispiele:*

- $(A_1 \wedge \neg A_2 \wedge A_3) \vee (\neg A_2 \wedge \neg A_3) \vee (A_2 \wedge A_1)$  ist in DNF
- $A_1 \vee \neg A_2 \vee A_3$  ist in DNF (mit  $n = 3$  und  $m_1 = m_2 = m_3 = 1$ )
- $A_1 \wedge \neg A_2 \wedge A_3$  ist in DNF (mit  $n = 1$  und  $m_1 = 3$ ) und gleichzeitig ist diese Formel eine konjunktive Klausel

Folie 111

- (c) Eine Formel ist in *konjunktiver Normalform (KNF)*, wenn sie eine Konjunktion von Disjunktion von Literalen ist, d.h., wenn sie die Form

$$\bigwedge_{i=1}^n \left( \bigvee_{j=1}^{m_i} \lambda_{i,j} \right)$$

hat, wobei  $n, m_1, \dots, m_n \geq 1$  sind und die  $\lambda_{i,j}$  für alle  $i \in [n]$  und  $j \in [m_i]$  Literale sind.

Die Subformeln  $\kappa_i := \bigvee_{j=1}^{m_i} \lambda_{i,j}$ , für  $i \in [n]$ , nennen wir die (*disjunktiven*) *Klauseln* der Formel.

*Beispiele:*

- $(A_1 \vee \neg A_2 \vee A_3) \wedge (\neg A_2 \vee \neg A_3) \wedge (A_2 \vee A_1)$  ist in KNF

- $A_1 \vee \neg A_2 \vee A_3$  ist in KNF (mit  $n = 1$  und  $m_1 = 3$ ) und gleichzeitig ist diese Formel eine disjunktive Klausel
- $A_1 \wedge \neg A_2 \wedge A_3$  ist in KNF (mit  $n = 3$  und  $m_1 = m_2 = m_3 = 1$ )

Folie 112

Normalformen spielen in vielen Anwendungsgebieten eine wichtige Rolle. Beispielsweise geht man in der Schaltungstechnik (Hardware-Entwurf) oft von DNF-Formeln aus, während bei der aussagenlogischen Modellbildung oftmals KNF-Formeln auftreten, da sich eine Sammlung von einfach strukturierten Aussagen sehr gut durch eine Konjunktion von Klauseln ausdrücken lässt.

Folie 113

**Satz 2.41.** *Jede aussagenlogische Formel ist äquivalent zu einer Formel in DNF und zu einer Formel in KNF.*

*Beweis.* Sei  $\psi$  eine Formel.

*DNF:* Falls  $\psi$  unerfüllbar ist, so ist  $\psi \equiv X \wedge \neg X$  (für jedes  $X \in \text{AS}$ ). Die Formel  $X \wedge \neg X$  ist sowohl in KNF als auch in DNF.

Falls  $\psi$  erfüllbar ist, so liefert der Beweis von Satz 2.30, angewendet auf die Wahrheitstafel von  $\psi$  (bzw. die von  $\psi$  berechnete boolesche Funktion), eine zu  $\psi$  äquivalente Formel in DNF (Details: Übung).

*KNF:* Sei  $\tilde{\psi}$  die zu  $\psi$  duale Formel. Man beachte, dass  $\tilde{\tilde{\psi}} = \psi$ .

Sei  $\varphi$  eine zu  $\tilde{\psi}$  äquivalente Formel in DNF (dass es eine solche Formel gibt, haben wir gerade bereits gezeigt), und sei  $\tilde{\varphi}$  die zu  $\varphi$  duale Formel. Dann ist  $\tilde{\varphi}$  offensichtlich in KNF. Und da

$$\tilde{\psi} \equiv \varphi$$

ist, gilt gemäß dem Dualitätssatz der Aussagenlogik (Satz 2.27), dass

$$\tilde{\tilde{\psi}} \equiv \tilde{\varphi}.$$

Wegen  $\tilde{\tilde{\psi}} = \psi$  ist  $\psi$  also äquivalent zur KNF-Formel  $\tilde{\varphi}$ .

□

**Bemerkung 2.42.** Der Beweis von Satz 2.41 zeigt Folgendes:  
Um für eine gegebene Formel  $\psi$  eine äquivalente Formel  $\varphi$  in

- DNF zu erzeugen, können wir die Wahrheitstafel für  $\psi$  aufstellen und dann wie in Beispiel 2.32 vorgehen (bzw.  $\varphi := A_1 \wedge \neg A_1$  setzen, falls  $\psi$  unerfüllbar ist).
- KNF zu erzeugen, können wir wie folgt vorgehen:
  - (1) Stelle die Wahrheitstafel für  $\psi$  auf.
  - (2) Falls in der letzten Spalte nur „1“en stehen, setze  $\varphi := A_1 \vee \neg A_1$ .
  - (3) Ansonsten gehe wie folgt vor:
    - Betrachte alle Zeilen der Wahrheitstafel, bei denen in der letzten Spalte eine „0“ steht.
    - Für jede solche Zeile konstruiere die disjunktive Klausel, die von allen Interpretationen außer der zur Zeile gehörenden erfüllt wird.

*Beispiel:* Wenn die Zeile der Wahrheitstafel die Form

$$0 \ 1 \ 1 \ | \ 0$$

hat, so gehört dazu die disjunktive Klausel

$$A_1 \vee \neg A_2 \vee \neg A_3.$$

- Bilde die Konjunktion all dieser disjunktiven Klauseln.  
Dies liefert die gesuchte KNF-Formel  $\varphi$ .

Wenn eine Formel sehr viele verschiedene Aussagensymbole enthält, die zur Formel gehörige Wahrheitstafel also sehr groß ist, ist das gerade beschriebene Verfahren zur Umformung in DNF oder KNF sehr zeitaufwändig. In solchen Fällen ist es ratsam, stattdessen zu versuchen, die gewünschte Normalform durch Äquivalenzumformungen zu erzeugen.

**Beispiel 2.43.** Sei  $\varphi := ((\neg A_0 \wedge (A_0 \rightarrow A_1)) \vee (A_2 \rightarrow A_3))$ .

Transformation von  $\varphi$  in NNF:

$$\left( (\neg A_0 \wedge (A_0 \Rightarrow A_1)) \vee (A_2 \Rightarrow A_3) \right) \equiv \underbrace{\left( (\neg A_0 \wedge (\neg A_0 \vee A_1)) \vee (\neg A_2 \vee A_3) \right)}_{=: \varphi'}$$

Transformation in DNF:

Wir betrachten die NNF-Formel

$$\varphi' = \left( (\underline{\neg A_0} \wedge (\underline{\neg A_0} \vee A_1)) \vee (\neg A_2 \vee A_3) \right).$$

und wenden die Distributivitätsregel (Satz 2.25(e)) auf die unterstrichene Subformel von  $\varphi'$  an. Dies liefert die Formel

$$\varphi'' := \left( ((\underline{\neg A_0} \wedge \underline{\neg A_0}) \vee (\underline{\neg A_0} \wedge A_1)) \vee (\neg A_2 \vee A_3) \right).$$

Diese Formel ist in DNF (die einzelnen konjunktiven Klauseln sind jeweils unterstrichen).

Transformation in KNF:

Wir betrachten die NNF-Formel

$$\varphi' = \left( (\underline{\neg A_0} \wedge (\underline{\neg A_0} \vee A_1)) \underline{\vee} (\neg A_2 \vee A_3) \right).$$

und wenden die Distributivitätsregel (Satz 2.25(e)) auf den unterstrichenen Teil der Formel  $\varphi'$  an. Dies liefert die Formel

$$\varphi'' := \left( (\underline{\neg A_0} \vee (\neg A_2 \vee A_3)) \wedge ((\underline{\neg A_0} \vee A_1) \underline{\vee} (\neg A_2 \vee A_3)) \right).$$

Dies ist eine KNF-Formel (die einzelnen disjunktiven Klauseln sind jeweils unterstrichen).

Je nach Formel muss man ggf. die Distributivitätsregel mehrmals anwenden, bis man eine Formel der gewünschten Normalform erhält.

## Ein DNF-Algorithmus

**Eingabe:** Formel  $\varphi \in \text{AL}(\{\neg, \wedge, \vee\})$  in NNF.

**Ausgabe:** Formel  $\varphi''$  in DNF

**Verfahren:**

1. Wiederhole folgende Schritte:
2. Wenn  $\varphi$  in DNF ist, dann halte mit Ausgabe  $\varphi$ .
3. Ersetze eine Subformel von  $\varphi$  der Gestalt  $(\psi_1 \wedge (\psi_2 \vee \psi_3))$  durch  $((\psi_1 \wedge \psi_2) \vee (\psi_1 \wedge \psi_3))$  oder eine Subformel der Gestalt  $((\psi_1 \vee \psi_2) \wedge \psi_3)$  durch  $((\psi_1 \wedge \psi_3) \vee (\psi_2 \wedge \psi_3))$ . Sei  $\varphi'$  die resultierende Formel.
4.  $\varphi := \varphi'$ .

**Satz 2.44.** Für jede Eingabeformel  $\varphi$  in NNF gibt der DNF-Algorithmus nach endlich vielen Schritten eine zu  $\varphi$  äquivalente Formel  $\varphi''$  in DNF aus.

(hier ohne Beweis)

Analog kann man auch einen „KNF-Algorithmus“ angeben, der bei Eingabe einer NNF-Formel eine äquivalente Formel in KNF erzeugt (Details: Übung).

Folie 118

## Eine kleine Formel mit großer DNF

Die Transformation einer Formel in eine äquivalente DNF- oder KNF-Formel kann u.U. allerdings sehr lang dauern, da es einige Formeln gibt, zu denen äquivalente DNF-Formeln zwangsläufig sehr groß sind. Dies wird durch den folgenden Satz präzisiert.

**Satz 2.45.** Sei  $n \in \mathbb{N}$  mit  $n \geq 1$ , seien  $X_1, \dots, X_n$  und  $Y_1, \dots, Y_n$  genau  $2n$  verschiedene Aussagensymbole und sei

$$\varphi_n := \bigwedge_{i=1}^n (X_i \vee \neg Y_i).$$

Jede zu  $\varphi_n$  äquivalente Formel in DNF hat mindestens  $2^n$  konjunktive Klauseln.



Beweis: Übung

**Korollar 2.46.** *Jeder Algorithmus, der bei Eingabe von beliebigen aussagenlogischen Formeln dazu äquivalente Formeln in DNF erzeugt, hat eine Laufzeit, die im worst-case exponentiell ist, d.h.,  $2^{\Omega(n)}$  bei Eingabe von Formeln der Länge  $n$ .*

## 2.5 Der Endlichkeitssatz

Folie 119

### Der Endlichkeitssatz (auch bekannt als Kompaktheitssatz)

Um nachzuweisen, dass eine gegebene *unendliche* Formelmenge erfüllbar ist, ist der folgende Satz sehr nützlich.

**Satz 2.47** (Der Endlichkeitssatz der Aussagenlogik).

(a) Für jede Formelmenge  $\Phi \subseteq \text{AL}$  gilt:

$\Phi$  ist erfüllbar  $\iff$  Jede endliche Teilmenge von  $\Phi$  ist erfüllbar.

(b) Für alle  $\Phi \subseteq \text{AL}$  und  $\psi \in \text{AL}$  gilt:

$\Phi \models \psi \iff$  Es gibt eine endliche Teilmenge  $\Gamma$  von  $\Phi$ , so dass  $\Gamma \models \psi$ .

*Beweis von (b) unter Verwendung von (a):*

Es gilt

$$\begin{aligned} \Phi \models \psi &\iff \Phi \cup \{\neg\psi\} \text{ ist unerfüllbar} && \text{(Lemma 2.19)} \\ &\iff \text{es gibt eine endliche Teilmenge} && \text{(Endlichkeitssatz)} \\ &\quad \Gamma \text{ von } \Phi, \text{ so dass} \\ &\quad \Gamma \cup \{\neg\psi\} \text{ unerfüllbar ist} \\ &\iff \text{es gibt eine endliche Teilmenge} && \text{(Lemma 2.19).} \\ &\quad \Gamma \text{ von } \Phi, \text{ so dass } \Gamma \models \psi \end{aligned}$$

□

*Beweis von Satz 2.47(a).*

Die Richtung „ $\implies$ “ ist offensichtlich, denn eine Interpretation, die  $\Phi$  erfüllt, erfüllt auch jede Teilmenge von  $\Phi$ .

Für die Richtung „ $\impliedby$ “ sei jede endliche Teilmenge von  $\Phi$  erfüllbar. Ziel ist, zu zeigen, dass es eine Interpretation gibt, die alle Formeln in  $\Phi$  erfüllt.

Zunächst definieren wir dazu rekursiv für alle  $i \in \mathbb{N}$  eine Menge  $\Psi_i$ . Wir starten mit  $\Psi_0 := \Phi$  und wählen für alle  $i \in \mathbb{N}$  die Menge  $\Psi_{i+1}$  wie folgt (zur Erinnerung:  $\text{AS} = \{A_0, A_1, A_2, \dots\}$ ):

- Falls jede endliche Teilmenge von  $\Psi_i \cup \{A_i\}$  erfüllbar ist, so setze  $\Psi_{i+1} := \Psi_i \cup \{A_i\}$ ,
- ansonsten, falls jede endliche Teilmenge von  $\Psi_i \cup \{\neg A_i\}$  erfüllbar ist, setze  $\Psi_{i+1} := \Psi_i \cup \{\neg A_i\}$ ,
- ansonsten setze  $\Psi_{i+1} := \Psi_i$ .

Sei weiterhin

$$\Psi := \bigcup_{i \in \mathbb{N}} \Psi_i.$$

Offensichtlicherweise gilt

$$\Phi = \Psi_0 \subseteq \Psi_1 \subseteq \Psi_2 \subseteq \Psi_3 \subseteq \dots \subseteq \Psi.$$

*Behauptung 1.*

Für jedes  $i \in \mathbb{N}$  gilt: Jede endliche Teilmenge von  $\Psi_i$  ist erfüllbar.

*Beweis.* Per Induktion nach  $i$ .

$i = 0$ : Es gilt  $\Psi_0 = \Phi$ , und nach Voraussetzung ist jede endliche Teilmenge von  $\Phi$  erfüllbar.

$i \rightarrow i+1$ : Falls  $\Psi_{i+1} = \Psi_i$ , so ist gemäß Induktionsannahme jede endliche Teilmenge von  $\Psi_{i+1}$  erfüllbar. Ansonsten ist per Definition von  $\Psi_{i+1}$  jede endliche Teilmenge von  $\Psi_{i+1}$  erfüllbar.  $\square_{Beh.1}$

*Behauptung 2.*

Jede endliche Teilmenge von  $\Psi$  ist erfüllbar.

*Beweis.* Jede endliche Teilmenge von  $\Psi$  ist in einem  $\Psi_i$  (für ein  $i \in \mathbb{N}$ ) enthalten und daher gemäß Behauptung 1 erfüllbar.  $\square_{Beh.2}$

*Behauptung 3.*

Für jedes  $n \in \mathbb{N}$  gilt:  $A_n \in \Psi$  oder  $\neg A_n \in \Psi$  (aber nicht beides, weil gemäß Behauptung 2 jede endliche Teilmenge von  $\Psi$  erfüllbar ist).

*Beweis. Angenommen*, die Behauptung ist falsch. Dann gibt es ein  $n \in \mathbb{N}$ , so dass weder  $A_n$  noch  $\neg A_n$  zur Menge  $\Psi$  gehört.

Gemäß der Definition der Mengen  $\Psi$  und  $\Psi_i$  für  $i \in \mathbb{N}$  gilt dann:  $A_n \notin \Psi_{n+1}$  und  $\neg A_n \notin \Psi_{n+1}$ . Daher gibt es gemäß der Definition von  $\Psi_{n+1}$  also endliche Teilmengen  $\Gamma_+$  und  $\Gamma_-$  von  $\Psi_n$ , so dass weder  $\Gamma_+ \cup \{A_n\}$  noch  $\Gamma_- \cup \{\neg A_n\}$  erfüllbar ist.

Weil  $\Gamma_+ \cup \Gamma_-$  eine endliche Teilmenge von  $\Psi_n$  ist, ist  $\Gamma_+ \cup \Gamma_-$  gemäß Behauptung 1 erfüllbar. Sei also  $\mathcal{I}$  ein Modell von  $\Gamma_+ \cup \Gamma_-$ . Falls  $\mathcal{I}(A_n) = 1$ , so gilt  $\mathcal{I} \models \Gamma_+ \cup \{A_n\}$ . Falls  $\mathcal{I}(A_n) = 0$ , so gilt  $\mathcal{I} \models \Gamma_- \cup \{\neg A_n\}$ . Also ist doch eine der beiden Mengen erfüllbar. *Widerspruch.*  $\square_{Beh.3}$

Gemäß Behauptung 3 können wir nun eine Interpretation  $\mathcal{I} : \mathcal{AS} \rightarrow \{0, 1\}$  definieren, indem wir für alle  $i \in \mathbb{N}$  setzen:

$$\mathcal{I}(A_i) := \begin{cases} 1 & \text{falls } A_i \in \Psi, \\ 0 & \text{falls } \neg A_i \in \Psi. \end{cases}$$

*Behauptung 4.*

$$\mathcal{I} \models \Psi.$$

*Beweis. Angenommen*, die Behauptung ist falsch. Dann gibt es eine Formel  $\psi \in \Psi$ , so dass  $\mathcal{I} \not\models \psi$ . Wähle  $n \in \mathbb{N}$  so, dass in  $\psi$  nur Aussagensymbole aus  $\{A_0, A_1, \dots, A_n\}$  vorkommen. Für  $i \in \{0, 1, \dots, n\}$  sei  $\varphi_i := A_i$  falls  $A_i \in \Psi$ , und  $\varphi_i := \neg A_i$  falls  $\neg A_i \in \Psi$ . Dann ist  $\Gamma := \{\psi, \varphi_0, \varphi_1, \dots, \varphi_n\}$  eine endliche Teilmenge von  $\Psi$  und daher gemäß Behauptung 2 erfüllbar. Sei  $\mathcal{J}$  also ein Modell von  $\Gamma$ . Für jedes  $i \in \{0, 1, \dots, n\}$  gilt  $\mathcal{J} \models \varphi_i$ , und daher  $\mathcal{J}(A_i) = \mathcal{I}(A_i)$ . Wegen  $\mathcal{J} \models \psi$  folgt aus dem Koinzidenzlemma, dass  $\mathcal{I} \models \psi$ . *Widerspruch.*  $\square_{Beh.4}$

Gemäß Behauptung 4 ist  $\mathcal{I}$  ein Modell von  $\Psi$  und wegen  $\Phi \subseteq \Psi$  auch ein Modell von  $\Phi$ . Daher ist  $\Phi$  erfüllbar.  $\square$

## Anwendung: Färbbarkeit

*Definition:*

- Ein (*ungerichteter*) Graph  $G = (V, E)$  besteht aus einer nicht-leeren Menge  $V$  und einer Menge  $E \subseteq \{\{x, y\} : x, y \in V, x \neq y\}$ . Die Elemente in  $V$  werden *Knoten* und die Elemente in  $E$  werden (*ungerichtete*) *Kanten* genannt. Zwei Knoten  $x, y \in V$  heißen *benachbart*, wenn  $\{x, y\} \in E$ .
- Ein *Subgraph* eines Graphen  $G = (V, E)$  ist ein Graph  $H = (V', E')$  mit  $V' \subseteq V$  und  $E' \subseteq E$ .
- Ein Graph  $G = (V, E)$  heißt *endlich* (bzw. *unendlich*), wenn seine Knotenmenge  $V$  endlich (bzw. unendlich) ist.

**Beispiel:**

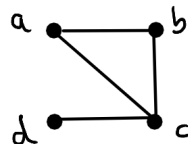
- $G_1 := (V_1, E_1)$  mit

$$V_1 = \{a, b, c, d\} \quad \text{und} \quad E_1 = \{\{a, b\}, \{b, c\}, \{c, d\}, \{a, c\}\}$$

ist ein Graph. Dieser Graph ist endlich. Die Knoten  $a$  und  $c$  sind benachbart, die Knoten  $a$  und  $d$  sind nicht benachbart.

Graphen werden i.d.R. dadurch illustriert, dass man die einzelnen Knoten als Punkte und die Kanten als Linien zwischen den Punkten zeichnet.

*Skizze:*



- $G_2 := (V_2, E_2)$  mit  $V_2 := \mathbb{N}$  und

$$E_2 := \{\{x, y\} : x, y \in \mathbb{N}_{\geq 1}, x \neq y, \text{ es gibt ein } z \in \mathbb{N}_{\geq 1} \text{ s.d. } y = x \cdot z\}$$

ist ein Graph. Dieser Graph ist unendlich. Der Knoten 0 ist mit keinem Knoten benachbart. Der Knoten 2 ist mit allen Knoten  $n \neq 2$  benachbart, für die gilt:  $n \neq 0$  und  $n$  ist eine gerade Zahl.

**Definition 2.48.** Sei  $k \in \mathbb{N}$  mit  $k \geq 1$ .

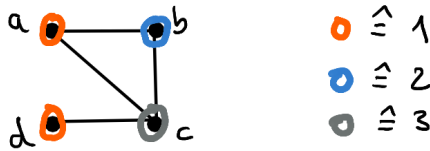
Eine *k-Färbung* eines Graphen  $G = (V, E)$  ist eine Abbildung  $f : V \rightarrow [k]$ , so dass für alle Kanten  $\{v, w\} \in E$  gilt:  $f(v) \neq f(w)$ .

$G$  heißt *k-färbbar*, falls es eine *k-Färbung* von  $G$  gibt.

**Beispiel:**

- Der Graph  $G_1$  ist nicht 2-färbbar. Aber er ist 3-färbbar; beispielsweise ist die Abbildung  $f : V_1 \rightarrow \{1, 2, 3\}$  mit  $f(a) = f(d) = 1$ ,  $f(b) = 2$  und  $f(c) = 3$  eine 3-Färbung von  $G_1$ .

Skizze:



- Für alle  $k \in \mathbb{N}_{\geq 1}$  gilt:  $G_2$  ist nicht  $k$ -färbbar.

*Beweis:* Übung!

**Satz 2.49.** Sei  $k \in \mathbb{N}$  mit  $k \geq 1$ .

Ein unendlicher Graph  $G$  mit Knotenmenge  $\mathbb{N}$  ist genau dann  $k$ -färbbar, wenn jeder endliche Subgraph von  $G$   $k$ -färbbar ist.

*Beweis.* Sei  $k \in \mathbb{N}$  mit  $k \geq 1$  und sei  $G = (V, E)$  ein unendlicher Graph mit Knotenmenge  $V = \mathbb{N}$ .

Zum Beweis des Satzes bilden wir ein aussagenlogisches Modell und wenden den Endlichkeitssatz an. Wir betrachten dazu

- Aussagensymbole  $X_{v,i}$  für alle  $v \in V$  und  $i \in [k]$ , die besagen: „Knoten  $v$  erhält Farbe  $i$ .“
- für jeden Knoten  $v \in V$  eine Formel

$$\varphi_v := \bigvee_{i \in [k]} ( X_{v,i} \wedge \bigwedge_{\substack{j \in [k] \\ j \neq i}} \neg X_{v,j} ),$$

die besagt: „Knoten  $v$  erhält genau eine Farbe.“

- für jede Kante  $\{v, w\} \in E$  eine Formel

$$\psi_{\{v,w\}} := \bigwedge_{i=1}^k \neg (X_{v,i} \wedge X_{w,i}),$$

die besagt: „Benachbarte Knoten erhalten verschiedene Farben.“

Für jeden Subgraphen  $H = (V', E')$  von  $G$  sei

$$\Phi_H := \{ \varphi_v : v \in V' \} \cup \{ \psi_{\{v,w\}} : \{v,w\} \in E' \}.$$

Man sieht leicht, dass gilt:

$$\Phi_H \text{ ist erfüllbar} \iff H \text{ ist } k\text{-färbbar.} \quad (2.1)$$

Falls  $H$  endlich ist, so ist auch  $\Phi_H$  endlich. Außerdem gibt es für jede endliche Teilmenge  $\Gamma$  von  $\Phi_G$  einen endlichen Subgraphen  $H$  von  $G$ , so dass  $\Gamma \subseteq \Phi_H$ . Daher gilt:

$$\begin{array}{l} \text{Jede endliche Teilmenge} \\ \text{von } \Phi_G \text{ ist erfüllbar.} \end{array} \iff \begin{array}{l} \text{Für jeden endlichen Sub-} \\ \text{graphen } H \text{ von } G \text{ ist } \Phi_H \\ \text{erfüllbar.} \end{array} \quad (2.2)$$

Insgesamt erhalten wir:

$$\begin{array}{l} G \text{ ist } k\text{-färbbar} \\ \iff \Phi_G \text{ ist erfüllbar} \quad (2.1) \\ \iff \text{jede endliche Teilmenge von } \Phi_G \quad (\text{Endlichkeitssatz}) \\ \text{ist erfüllbar} \\ \iff \text{für jeden endlichen Subgraphen} \quad (2.2) \\ H \text{ von } G \text{ ist } \Phi_H \text{ erfüllbar} \\ \iff \text{jeder endliche Subgraph } H \text{ von } G \quad (2.1). \\ \text{ist } k\text{-färbbar} \end{array}$$

□

## 2.6 Resolution

Folie 121

Um nachzuweisen, dass eine gegebene KNF-Formel *unerfüllbar* ist, ist das im Folgenden vorgestellte Resolutionsverfahren nützlich.

**Beispiel 2.50.** Wir wollen nachweisen, dass die KNF-Formel

$$\varphi := (\neg P \vee \neg R) \wedge (P \vee \neg R) \wedge (\neg Q \vee S) \wedge (Q \vee R \vee T) \wedge \neg T \wedge (\neg S \vee R)$$

*unerfüllbar* ist. Dazu können wir wie folgt argumentieren:

Angenommen, eine Interpretation  $\mathcal{I}$  erfüllt  $\varphi$ .

- Dann gilt  $\mathcal{I} \models \neg T$ .
- Aus  $\mathcal{I} \models Q \vee R \vee T$  und  $\mathcal{I} \models \neg T$  folgt dann  $\mathcal{I} \models Q \vee R$ .

- Aus  $\mathcal{I} \models Q \vee R$  und  $\mathcal{I} \models \neg Q \vee S$  folgt  $\mathcal{I} \models R \vee S$ .
  - Aus  $\mathcal{I} \models R \vee S$  und  $\mathcal{I} \models \neg S \vee R$  folgt  $\mathcal{I} \models R$ .
  - Aus  $\mathcal{I} \models \neg P \vee \neg R$  und  $\mathcal{I} \models P \vee \neg R$  folgt  $\mathcal{I} \models \neg R$ .
- Das ist ein *Widerspruch*. Somit ist  $\varphi$  *nicht* erfüllbar.

Folie 122

## Umwandlung in kleine KNF-Formeln

Das Resolutionsverfahren, das wir im Folgenden vorstellen, funktioniert nur für KNF-Formeln.

*Wir wissen bereits:*

- Zu jeder Formel  $\varphi$  gibt es eine äquivalente Formel in KNF.
- Aber möglicherweise ist die kleinste zu  $\varphi$  äquivalente KNF-Formel exponentiell groß in der Größe von  $\varphi$ .

Wenn es uns nur um die Frage geht, ob eine Formel  $\varphi$  (*un*)*erfüllbar* ist, ist es aber auch gar nicht nötig, eine zu  $\varphi$  *äquivalente* KNF-Formel zu finden. Es reicht, eine zu  $\varphi$  *erfüllbarkeitsäquivalente* KNF-Formel zu konstruieren.

**Definition 2.51.** Zwei Formeln  $\varphi$  und  $\psi$  heißen *erfüllbarkeitsäquivalent*, falls gilt:

$$\varphi \text{ ist erfüllbar} \iff \psi \text{ ist erfüllbar.}$$

Folie 123

Eine beliebige Formel in eine *erfüllbarkeitsäquivalente* KNF-Formel umzuwandeln, ist in Linearzeit möglich.

**Beispiel 2.52.** Um die Formel

$$\varphi := (P \rightarrow \neg Q) \vee (\neg(P \wedge Q) \wedge R)$$

in eine erfüllbarkeitsäquivalente KNF-Formel umzuformen, können wir wie folgt vorgehen.

1. *Schritt*: Wir listen alle Subformeln von  $\varphi$  auf, die keine Literale sind:

$$\varphi := \underbrace{(P \rightarrow \neg Q)}_{\psi_1} \vee \underbrace{\left( \underbrace{\neg(P \wedge Q)}_{\psi_4} \wedge R \right)}_{\psi_2}.$$

Für jede Subformel  $\psi$  von  $\varphi$  sei  $X_\psi$  ein neues Aussagensymbol, das die Aussage „die Subformel  $\psi$  ist wahr“ repräsentiert.

Wir wählen

$$\begin{aligned} \varphi' := & X_\varphi \\ & \wedge (X_\varphi \leftrightarrow (X_{\psi_1} \vee X_{\psi_2})) && \text{(da } \varphi = (\psi_1 \vee \psi_2)\text{)} \\ & \wedge (X_{\psi_1} \leftrightarrow (P \rightarrow \neg Q)) && \text{(da } \psi_1 = (P \rightarrow \neg Q)\text{)} \\ & \wedge (X_{\psi_2} \leftrightarrow (X_{\psi_3} \wedge R)) && \text{(da } \psi_2 = (\psi_3 \wedge R)\text{)} \\ & \wedge (X_{\psi_3} \leftrightarrow \neg X_{\psi_4}) && \text{(da } \psi_3 = \neg\psi_4\text{)} \\ & \wedge (X_{\psi_4} \leftrightarrow (P \wedge Q)) && \text{(da } \psi_4 = (P \wedge Q)\text{)} \end{aligned}$$

Man sieht leicht, dass gilt:

$$\varphi \text{ ist erfüllbar} \iff \varphi' \text{ ist erfüllbar.}$$

2. *Schritt*: Die im 1. Schritt konstruierte Formel  $\varphi'$  ist eine Konjunktion von Teilformeln mit jeweils höchstens 3 Aussagensymbolen. Wir wandeln jetzt jede dieser Teilformeln in eine äquivalente KNF-Formel um und erhalten damit auch insgesamt eine zu  $\varphi'$  äquivalente KNF-Formel

$$\begin{aligned} \varphi_K := & X_\varphi \\ & \wedge (\neg X_\varphi \vee X_{\psi_1} \vee X_{\psi_2}) \wedge (X_\varphi \vee \neg X_{\psi_1}) \wedge (X_\varphi \vee \neg X_{\psi_2}) \\ & \wedge (\neg X_{\psi_1} \vee \neg P \vee \neg Q) \wedge (P \vee X_{\psi_1}) \wedge (Q \vee X_{\psi_1}) \\ & \wedge (\neg X_{\psi_2} \vee X_{\psi_3}) \wedge (\neg X_{\psi_2} \vee R) \wedge (\neg X_{\psi_3} \vee \neg R \vee X_{\psi_2}) \\ & \wedge (\neg X_{\psi_3} \vee \neg X_{\psi_4}) \wedge (X_{\psi_4} \vee X_{\psi_3}) \\ & \wedge (\neg X_{\psi_4} \vee P) \wedge (\neg X_{\psi_4} \vee Q) \wedge (\neg P \vee \neg Q \vee X_{\psi_4}). \end{aligned}$$

Da  $\varphi_K$  äquivalent zu  $\varphi'$  und  $\varphi'$  erfüllbarkeitsäquivalent zu  $\varphi$  ist, ist insgesamt  $\varphi_K$  erfüllbarkeitsäquivalent zu  $\varphi$ .



## Das Tseitin-Verfahren

Auf die gleiche Weise wie in Beispiel 2.52 können wir jede beliebige aussagenlogische Formel in eine erfüllbarkeitsäquivalente KNF-Formel umwandeln. Dieses Verfahren wird *Tseitin-Verfahren* genannt. Eine Laufzeitanalyse zeigt, dass das Tseitin-Verfahren in Linearzeit durchgeführt werden kann. Insgesamt erhalten wir so den folgenden Satz.

**Satz 2.53.** *Es gibt eine Zahl  $c \in \mathbb{N}_{\geq 1}$ , so dass gilt:*

*Zu jeder aussagenlogischen Formel  $\varphi$  gibt es eine aussagenlogische Formel  $\varphi_K$  mit folgenden Eigenschaften:*

(a)  $\varphi_K$  ist erfüllbarkeitsäquivalent zu  $\varphi$ .

(b)  $\varphi_K$  ist in 3-KNF, d.h., in KNF, wobei jede disjunktive Klausel aus höchstens 3 Literalen besteht (wir sagen: die Klauseln haben Länge  $\leq 3$ ).

(c)  $|\varphi_K| \leq c \cdot |\varphi|$ .

Außerdem gibt es einen Algorithmus, der  $\varphi_K$  bei Eingabe von  $\varphi$  in Linearzeit berechnet.

Beweis: Übung.

**Notation.**  $|\varphi|$  bezeichnet die *Länge* (bzw. *Größe*) einer aussagenlogischen Formel  $\varphi$ , d.h. die Länge von  $\varphi$  aufgefasst als Wort über dem Alphabet  $A_{AL}$ .

Folie 125

## Repräsentation von KNF-Formeln

Für den Rest diese Abschnitts werden wir nur noch KNF-Formeln betrachten, und wenn wir von *Klauseln* sprechen, meinen wir stets *disjunktive Klauseln*, also Disjunktionen von Literalen.

Für das Resolutionsverfahren ist die folgende Repräsentation von Klauseln und KNF-Formeln sehr hilfreich:

- Eine Klausel  $(\lambda_1 \vee \dots \vee \lambda_\ell)$ , die aus Literalen  $\lambda_1, \dots, \lambda_\ell$  besteht, identifizieren wir mit der Menge  $\{\lambda_1, \dots, \lambda_\ell\}$  ihrer Literale.

*Beispiel:* Wir schreiben z.B.  $\{A_1, \neg A_2, A_3\}$  um die Klausel  $(A_1 \vee \neg A_2 \vee A_3)$  zu bezeichnen.

D.h.: Ab jetzt sind disjunktive Klauseln für uns dasselbe wie endliche Mengen von Literalen. *Wenn wir von einer Klausel sprechen, meinen wir eine endliche Menge von Literalen* und identifizieren diese mit der Formel, die aus der Disjunktion all dieser Literale besteht.

*Spezialfall:* Die leere Menge  $\emptyset$  entspricht der unerfüllbaren Formel  $\mathbf{0}$  (die wiederum der „Formel“ entspricht, die aus der Disjunktion aller Literale aus  $\emptyset$  besteht).

Folie 126

- Eine KNF-Formel  $\varphi = \bigwedge_{i=1}^m \gamma_i$ , die aus (disjunktiven) Klauseln  $\gamma_1, \dots, \gamma_m$  besteht, identifizieren wir mit der Menge  $\Gamma := \{\gamma_1, \dots, \gamma_m\}$  ihrer Klauseln.

Offensichtlicherweise gilt für alle Interpretationen  $\mathcal{I}$ :

$$\mathcal{I} \models \varphi \iff \mathcal{I} \models \Gamma.$$

*Beispiel:* Die KNF-Formel  $\varphi = A_1 \wedge (\neg A_2 \vee A_1) \wedge (A_3 \vee \neg A_2 \vee \neg A_1)$  repräsentieren wir durch die endliche Klauselmenge

$$\{ A_1, (\neg A_2 \vee A_1), (A_3 \vee \neg A_2 \vee \neg A_1) \}$$

bzw. durch

$$\{ \{A_1\}, \{\neg A_2, A_1\}, \{A_3, \neg A_2, \neg A_1\} \}$$

„Erfüllbarkeit von KNF-Formeln“ ist damit im Wesentlichen dasselbe Problem wie „Erfüllbarkeit von endlichen Mengen von Klauseln“.

Folie 127

## Resolution

**Notation.** Für ein Literal  $\lambda$  sei

$$\bar{\lambda} := \begin{cases} \neg X, & \text{falls } \lambda \text{ von der Form } X \text{ für ein } X \in \text{AS} \text{ ist} \\ X, & \text{falls } \lambda \text{ von der Form } \neg X \text{ für ein } X \in \text{AS} \text{ ist.} \end{cases}$$

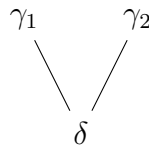
Wir nennen  $\bar{\lambda}$  auch das *Negat* von  $\lambda$ .

**Definition 2.54** (Resolutionsregel).

Seien  $\gamma_1, \gamma_2$  und  $\delta$  endliche Mengen von Literalen (d.h. disjunktive Klauseln). Dann ist  $\delta$  eine *Resolvente* von  $\gamma_1$  und  $\gamma_2$ , wenn es ein Literal  $\lambda$  gibt, so dass gilt:

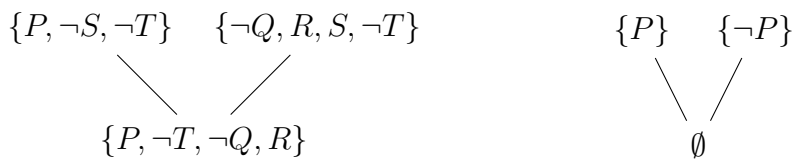
$$\lambda \in \gamma_1, \quad \bar{\lambda} \in \gamma_2 \quad \text{und} \quad \delta = (\gamma_1 \setminus \{\lambda\}) \cup (\gamma_2 \setminus \{\bar{\lambda}\}).$$

**Graphische Darstellung:**



„ $\delta$  ist eine Resolvente von  $\gamma_1$  und  $\gamma_2$ .“

**Beispiele.**



Folie 128

**Das Resolutionslemma**

**Notation.** Ein *Klausel* ist eine endliche Menge von Literalen (eine solche Klausel repräsentiert die Disjunktion der in ihr enthaltenen Literale). Eine *Klauselmenge* ist eine (endliche oder unendliche) Menge von Klauseln.

**Lemma 2.55** (Resolutionslemma). *Sei  $\Gamma$  eine Klauselmenge, seien  $\gamma_1, \gamma_2 \in \Gamma$  und sei  $\delta$  eine Resolvente von  $\gamma_1$  und  $\gamma_2$ . Dann sind die Klauselmengen  $\Gamma$  und  $\Gamma \cup \{\delta\}$  äquivalent.*

*Beweis.* Sei  $\mathcal{I}$  eine beliebige Interpretation. Wir zeigen:

$$\mathcal{I} \models \Gamma \quad \iff \quad \mathcal{I} \models \Gamma \cup \{\delta\}.$$

„ $\iff$ “: Trivial.

„ $\implies$ “: Es gelte  $\mathcal{I} \models \Gamma$ . Wir müssen zeigen, dass auch gilt:  $\mathcal{I} \models \delta$ .

Da  $\delta$  eine Resolvente von  $\gamma_1$  und  $\gamma_2$  ist, gibt es ein Literal  $\lambda$ , so dass  $\delta = (\gamma_1 \setminus \{\lambda\}) \cup (\gamma_2 \setminus \{\bar{\lambda}\})$ .

*Fall 1:*  $\mathcal{I} \models \lambda$ .

Dann gilt:  $\mathcal{I} \not\models \bar{\lambda}$ . Wegen  $\mathcal{I} \models \gamma_2$ , muss es ein Literal  $\mu \in \gamma_2 \setminus \{\bar{\lambda}\} \subseteq \delta$  geben, so dass  $\mathcal{I} \models \mu$ . Also gilt  $\mathcal{I} \models \delta$ .

*Fall 2:*  $\mathcal{I} \not\models \lambda$ .

Wegen  $\mathcal{I} \models \gamma_1$ , muss es ein Literal  $\mu \in \gamma_1 \setminus \{\lambda\} \subseteq \delta$  geben, so dass  $\mathcal{I} \models \mu$ . Also gilt  $\mathcal{I} \models \delta$ .

In beiden Fällen gilt  $\mathcal{I} \models \delta$ . Insgesamt gilt also  $\mathcal{I} \models \Gamma \cup \{\delta\}$ .

□

Folie 129

## Resolutionsableitungen und -widerlegungen

**Definition 2.56.** Sei  $\Gamma$  eine Klauselmenge.

- (a) Eine *Resolutionsableitung* einer Klausel  $\delta$  aus  $\Gamma$  ist ein Tupel  $(\delta_1, \dots, \delta_\ell)$  von Klauseln, so dass gilt:  $\ell \geq 1$ ,  $\delta_\ell = \delta$ , und für alle  $i \in [\ell]$  ist
- $\delta_i \in \Gamma$ , oder
  - es gibt  $j, k \in [i-1]$ , so dass  $\delta_i$  eine Resolvente von  $\delta_j$  und  $\delta_k$  ist.
- (b) Eine *Resolutionswiderlegung* von  $\Gamma$  ist eine Resolutionsableitung der leeren Klausel aus  $\Gamma$ .

*Zur Erinnerung:*

Eine Klausel  $\delta$  ist genau dann eine *Resolvente* zweier Klauseln  $\gamma_1$  und  $\gamma_2$ , wenn es ein Literal  $\lambda$  gibt, so dass gilt:

$$\lambda \in \gamma_1, \quad \bar{\lambda} \in \gamma_2 \quad \text{und} \quad \delta = (\gamma_1 \setminus \{\lambda\}) \cup (\gamma_2 \setminus \{\bar{\lambda}\}).$$

Folie 130

**Notation 2.57.**

- (a) Wir schreiben kurz  $\Gamma \vdash_R \delta$  um auszudrücken, dass es eine Resolutionsableitung von  $\delta$  aus  $\Gamma$  gibt. Insbesondere bedeutet  $\Gamma \vdash_R \emptyset$ , dass es eine Resolutionswiderlegung von  $\Gamma$  gibt.

(b) An Stelle von  $(\delta_1, \dots, \delta_\ell)$  schreiben wir Resolutionsableitungen der besseren Lesbarkeit halber oft zeilenweise, also

- (1)  $\delta_1$
- (2)  $\delta_2$
- $\vdots$
- ( $\ell$ )  $\delta_\ell$

und geben am Ende jeder Zeile eine kurze Begründung an.

Folie 131

**Beispiel 2.58.** Sei

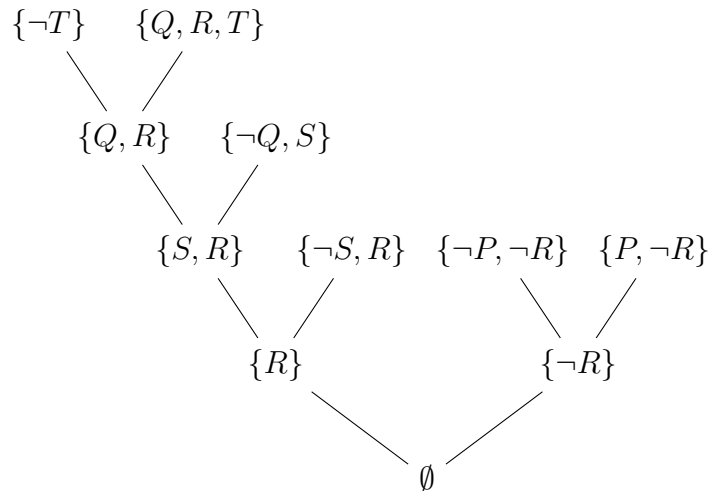
$$\Gamma := \{ \{ \neg P, \neg R \}, \{ P, \neg R \}, \{ \neg Q, S \}, \{ Q, R, T \}, \{ \neg T \}, \{ \neg S, R \}, \{ T, R \} \}$$

Eine Resolutionswiderlegung von  $\Gamma$  ist:

- (1)  $\{ \neg T \}$  (in  $\Gamma$ )
- (2)  $\{ Q, R, T \}$  (in  $\Gamma$ )
- (3)  $\{ Q, R \}$  (Resolvente von (1), (2))
- (4)  $\{ \neg Q, S \}$  (in  $\Gamma$ )
- (5)  $\{ S, R \}$  (Resolvente von (3), (4))
- (6)  $\{ \neg S, R \}$  (in  $\Gamma$ )
- (7)  $\{ R \}$  (Resolvente von (5), (6))
- (8)  $\{ \neg P, \neg R \}$  (in  $\Gamma$ )
- (9)  $\{ P, \neg R \}$  (in  $\Gamma$ )
- (10)  $\{ \neg R \}$  (Resolvente von (8), (9))
- (11)  $\emptyset$  (Resolvente von (7), (10))

Folie 132

## Graphische Darstellung der Resolutionswiderlegung



Folie 133

Eine weitere Resolutionswiderlegung von  $\Gamma$  ist:

- (1)  $\{\neg T\}$  (in  $\Gamma$ )
- (2)  $\{T, R\}$  (in  $\Gamma$ )
- (3)  $\{R\}$  (Resolvente von (1), (2))
- (4)  $\{P, \neg R\}$  (in  $\Gamma$ )
- (5)  $\{P\}$  (Resolvente von (3), (4))
- (6)  $\{\neg P, \neg R\}$  (in  $\Gamma$ )
- (7)  $\{\neg R\}$  (Resolvente von (5), (6))
- (8)  $\emptyset$  (Resolvente von (7), (3))

Folie 134

## Korrektheit und Vollständigkeit der Resolution

**Satz 2.59.** Für jede Klauselmenge  $\Gamma$  gilt:

$$\Gamma \vdash_R \emptyset \iff \Gamma \text{ ist unerfüllbar.}$$

*D.h.: Eine Klauselmenge hat genau dann eine Resolutionswiderlegung, wenn sie unerfüllbar ist.*

*Beweis.* Sei  $\Gamma$  eine Klauselmeng. Wir müssen zeigen:

$\Gamma$  hat eine Resolutionswiderlegung  $\iff \Gamma$  ist unerfüllbar.

„ $\implies$ “ („Korrektheit des Resolutionskalküls“):

Sei  $(\gamma_1, \dots, \gamma_\ell)$  eine Resolutionswiderlegung von  $\Gamma$ . Dann ist  $\gamma_\ell = \emptyset$ . Sei  $\Gamma_0 := \Gamma$  und  $\Gamma_i := \Gamma \cup \{\gamma_1, \dots, \gamma_i\}$  für alle  $i \in [\ell]$ . Per Induktion zeigen wir, dass für alle  $i \in \{0, \dots, \ell\}$  gilt:  $\Gamma \equiv \Gamma_i$ . Dann sind wir fertig, denn  $\Gamma_\ell$  ist unerfüllbar, weil es die leere Klausel  $\emptyset$  enthält.

$i = 0$ : Trivial.

$i \rightarrow i+1$ :

Falls  $\gamma_{i+1} \in \Gamma$ , so gilt  $\Gamma_{i+1} = \Gamma_i$ , und damit gilt trivialerweise  $\Gamma_{i+1} \equiv \Gamma_i$ .

Andernfalls gibt es  $j, k \in [i]$ , so dass  $\gamma_{i+1}$  eine Resolvente von  $\gamma_j$  und  $\gamma_k$  ist. Wegen  $\Gamma_{i+1} = \Gamma_i \cup \{\gamma_{i+1}\}$  folgt aus dem Resolutionslemma, dass  $\Gamma_{i+1} \equiv \Gamma_i$ . Da gemäß Induktionsannahme  $\Gamma \equiv \Gamma_i$  ist, folgt insgesamt, dass  $\Gamma \equiv \Gamma_{i+1}$ .

„ $\impliedby$ “ („Vollständigkeit des Resolutionskalküls“):

Wir zeigen zunächst folgende Behauptung:

*Behauptung 1:* Sei  $n \in \mathbb{N}$ , und sei  $\Gamma$  eine unerfüllbare Klauselmeng. die nur Aussagensymbole in  $\{A_i : 0 \leq i < n\}$  enthält.

Dann besitzt  $\Gamma$  eine Resolutionswiderlegung.

*Beweis:* Per Induktion nach  $n$ .

$n = 0$ :  $\Gamma$  ist eine unerfüllbare Klauselmeng., die kein(e) Aussagensymbol(e) enthält. Somit ist  $\Gamma = \{\emptyset\}$ . Insbesondere ist  $(\emptyset)$  eine Resolutionswiderlegung von  $\Gamma$ .

*Induktionsschritt:*  $n \rightarrow n+1$ .

Sei  $\Gamma$  eine unerfüllbare Klauselmeng. mit Aussagensymbolen in  $\{A_0, \dots, A_n\}$ .

Seien

$$\begin{aligned} \Gamma_+ &:= \{ \gamma \setminus \{A_n\} : \gamma \in \Gamma \text{ mit } \neg A_n \notin \gamma \}, \\ \Gamma_- &:= \{ \gamma \setminus \{\neg A_n\} : \gamma \in \Gamma \text{ mit } A_n \notin \gamma \}. \end{aligned}$$

Dann enthalten  $\Gamma_+$  und  $\Gamma_-$  nur Aussagensymbole aus  $\{A_0, \dots, A_{n-1}\}$ .

*Behauptung 2:*  $\Gamma_+$  ist unerfüllbar.

*Beweis:* Angenommen,  $\Gamma_+$  ist erfüllbar.

Sei  $\mathcal{I}_+$  ein Modell von  $\Gamma_+$ , d.h.  $\mathcal{I}_+ \models \Gamma_+$ .

Sei  $\mathcal{I}$  die Interpretation mit  $\mathcal{I}(A_n) := 0$  und  $\mathcal{I}(X) := \mathcal{I}_+(X)$  für alle  $X \in \text{AS} \setminus \{A_n\}$ .

Gemäß Koinzidenzlemma gilt dann:  $\mathcal{I} \models \Gamma_+$ .

Aus der Definition von  $\Gamma_+$  folgt, dass für alle  $\gamma \in \Gamma$  mit  $\neg A_n \notin \gamma$  gilt:  $\mathcal{I} \models \gamma$ .

Wegen  $\mathcal{I}(A_n) = 0$  gilt außerdem für alle  $\gamma \in \Gamma$  mit  $\neg A_n \in \gamma$ , dass  $\mathcal{I} \models \gamma$ .

Somit gilt:  $\mathcal{I} \models \Gamma$ . Das ist ein *Widerspruch*, denn  $\Gamma$  ist laut Voraussetzung unerfüllbar.  $\square_{Beh.2}$

*Behauptung 3:*  $\Gamma_-$  ist unerfüllbar.

*Beweis:* Analog zum Beweis von Behauptung 2.  $\square_{Beh.3}$

*Behauptung 4:* Es gilt:  $\Gamma \vdash_R \emptyset$  oder  $\Gamma \vdash_R \{A_n\}$ .

*Beweis:* Gemäß Behauptung 2 und der Induktionsannahme hat  $\Gamma_+$  eine Resolutionswiderlegung, etwa  $(\gamma_1^+, \dots, \gamma_\ell^+)$ . Per Induktion nach  $i$  definieren wir für jedes  $i \in [\ell]$  eine Klausel  $\gamma_i$  wie folgt:

- Falls  $\gamma_i^+ \in \Gamma_+ \cap \Gamma$ , so wähle  $\gamma_i := \gamma_i^+$ .  
Klar: Dann ist  $\gamma_i \in \Gamma$ .
- Falls  $\gamma_i^+ \in \Gamma_+ \setminus \Gamma$ , so wähle  $\gamma_i := \gamma_i^+ \cup \{A_n\}$ .  
Klar: Dann ist  $\gamma_i \in \Gamma$ .
- Ansonsten ist  $\gamma_i^+ = (\gamma_j^+ \setminus \{\lambda\}) \cup (\gamma_k^+ \setminus \{\bar{\lambda}\})$  für ein Literal  $\lambda$  und Zahlen  $j, k \in [i-1]$ . Wir wählen dann  $\gamma_i := (\gamma_j \setminus \{\lambda\}) \cup (\gamma_k \setminus \{\bar{\lambda}\})$ .

Für jedes  $i \in [\ell]$  gilt dann entweder  $\gamma_i = \gamma_i^+$  oder  $\gamma_i = \gamma_i^+ \cup \{A_n\}$ . Außerdem ist  $(\gamma_1, \dots, \gamma_\ell)$  eine Resolutionsableitung von  $\gamma_\ell$  aus  $\Gamma$ . Weil  $\gamma_\ell^+ = \emptyset$  ist, gilt  $\gamma_\ell = \emptyset$  oder  $\gamma_\ell = \{A_n\}$ .  $\square_{Beh.4}$

*Behauptung 5:* Es gilt:  $\Gamma \vdash_R \emptyset$  oder  $\Gamma \vdash_R \{\neg A_n\}$ .

*Beweis:* Analog zum Beweis von Behauptung 4 mit  $\Gamma_-$  an Stelle von  $\Gamma_+$ .  $\square_{Beh.5}$

Aus den Behauptungen 4 und 5 folgt  $\Gamma \vdash_R \emptyset$ , entweder direkt oder durch einmaliges Anwenden der Resolutionsregel auf die Klauseln  $\{A_n\}$  und  $\{\neg A_n\}$ . Damit ist Behauptung 1 bewiesen.  $\square_{Beh.1}$



Sei nun  $\Gamma$  eine beliebige unerfüllbare Klauselmenge. Gemäß Endlichkeitssatz (Satz 2.47) existiert eine endliche unerfüllbare Teilmenge  $\Gamma'$  von  $\Gamma$ . Wähle eine solche Menge  $\Gamma'$ . Dann gibt es ein  $n \in \mathbb{N}$ , so dass  $\Gamma'$  nur Aussagensymbole aus  $\{A_0, \dots, A_{n-1}\}$  enthält. Dann folgt aus Behauptung 1, dass  $\Gamma' \vdash_R \emptyset$ , und daher auch  $\Gamma \vdash_R \emptyset$ . □

Folie 135

### Vorsicht

Beim Anwenden der Resolutionsregel (Definition 2.54) darf immer nur ein Literal  $\lambda$  betrachtet werden.

*Beispiel:*

Betrachte die Klauselmenge  $\Gamma := \{\gamma_1, \gamma_2\}$  mit  $\gamma_1 := \{X, Y\}$  und  $\gamma_2 := \{\neg X, \neg Y\}$  (wobei  $X$  und  $Y$  zwei verschiedene Aussagensymbole sind).

Offensichtlicherweise wird  $\Gamma$  von jeder Interpretation  $\mathcal{I}$  mit  $\mathcal{I}(X) = 1$  und  $\mathcal{I}(Y) = 0$  erfüllt. Gemäß Satz 2.59 gibt es also keine Resolutionswiderlegung von  $\Gamma$ .

Gemäß der Resolutionsregel gibt es für  $\gamma_1$  und  $\gamma_2$  zwei verschiedene Resolventen: Indem man die Resolutionsregel mit  $\lambda := X$  anwendet, erhält man  $\{Y, \neg Y\}$  als Resolvente von  $\gamma_1$  und  $\gamma_2$ . Indem man die Resolutionsregel mit  $\lambda := Y$  anwendet, erhält man  $\{X, \neg X\}$  als Resolvente von  $\gamma_1$  und  $\gamma_2$ .

Beachten Sie, dass die Resolutionsregel es *nicht* erlaubt, sie in einem einzigen Schritt für zwei verschiedene Literale  $\lambda$  und  $\lambda'$  anzuwenden. Und das ist auch gut so, denn sonst könnte man aus  $\gamma_1 := \{X, Y\}$  und  $\gamma_2 := \{\neg X, \neg Y\}$  für  $\lambda := \{X\}$  und  $\lambda' := \{Y\}$  als Resolvente die Klausel

$$(\gamma_1 \setminus \{\lambda, \lambda'\}) \cup (\gamma_2 \setminus \{\bar{\lambda}, \bar{\lambda}'\})$$

herleiten, d.h. die Klausel

$$(\{X, Y\} \setminus \{X, Y\}) \cup (\{\neg X, \neg Y\} \setminus \{\neg X, \neg Y\}),$$

also die leere Klausel. Dann hätten wir also eine „Resolutionswiderlegung“ von  $\Gamma$ , obwohl  $\Gamma$  erfüllbar ist. D.h. Satz 2.59 würde nicht gelten, und Resolutionsableitungen wären nicht dazu geeignet, Klauselmengen auf Erfüllbarkeit zu testen.

Folie 136

## Der Satz von Haken

Für eine endliche Klauselmengenge  $\Gamma$  sei die *Größe* von  $\Gamma$  die Zahl

$$\|\Gamma\| := \sum_{\gamma \in \Gamma} |\gamma|,$$

wobei  $|\gamma|$  die Anzahl der Literale in  $\gamma$  bezeichnet.

Der folgende (schwer zu beweisende) Satz zeigt, dass es im Worst-Case exponentiell lange dauern kann, eine Resolutionswiderlegung zu finden.

**Satz 2.60** (Satz von Haken, 1985). *Es gibt Konstanten  $c, d > 0$  und endliche Klauselmengen  $\Gamma_n$  für  $n \geq 1$ , so dass für alle  $n \in \mathbb{N}$  mit  $n \geq 1$  gilt:*

1.  $\|\Gamma_n\| \leq n^c$ ,
2.  $\Gamma_n$  ist unerfüllbar, und
3. jede Resolutionswiderlegung von  $\Gamma_n$  hat Länge  $\geq 2^{dn}$ .

(Hier ohne Beweis)

## 2.7 Erfüllbarkeitsalgorithmen

Folie 137

### Das aussagenlogische Erfüllbarkeitsproblem

Wir betrachten im Folgenden Algorithmen für das

*Aussagenlogische Erfüllbarkeitsproblem:*

*Eingabe:* eine Formel  $\varphi \in \text{AL}$

*Ausgabe:* „erfüllbar“, falls  $\varphi$  erfüllbar ist;  
 „unerfüllbar“, sonst.

**Notation.** Im Folgenden bezeichnet  $n$  immer die Anzahl der in  $\varphi$  vorkommenden verschiedenen Aussagensymbole, und  $m := |\varphi|$  bezeichnet die Länge von  $\varphi$  (aufgefasst als Wort über dem Alphabet der Aussagenlogik).

Folie 138

## Varianten des Erfüllbarkeitsproblems

### Berechnen einer erfüllenden Interpretation:

Zusätzlich soll bei erfüllbaren Formeln noch ein Modell berechnet werden, d.h., ein Tupel  $(b_1, \dots, b_n) \in \{0, 1\}^n$ , so dass  $\varphi[b_1, \dots, b_n] = 1$ .

### Einschränkung auf KNF-Formeln:

Oft beschränkt man sich auf Eingabeformeln in KNF oder sogar 3-KNF. Das ist keine wesentliche Einschränkung, weil sich mit Hilfe des Tseitin-Verfahrens jede Formel in Linearzeit in eine erfüllbarkeitsäquivalente Formel in 3-KNF transformieren lässt (Satz 2.53). Das Erfüllbarkeitsproblem für Formeln in KNF bzw. 3-KNF bezeichnet man mit *SAT* bzw. *3-SAT*.

Folie 139

## Komplexität des Erfüllbarkeitsproblems

**Satz 2.61** (Satz von Cook und Levin,  $\approx 1971$ ).

*Das aussagenlogische Erfüllbarkeitsproblem (und sogar die Einschränkung 3-SAT) ist NP-vollständig.*

Die Komplexitätsklassen P und NP, der Begriff der NP-Vollständigkeit, sowie ein Beweis des Satzes von Cook und Levin werden in der Vorlesung *Einführung in die Theoretische Informatik* behandelt.

### Bemerkung.

- Wenn also  $P \neq NP$  ist (was allgemein vermutet wird), gibt es für das aussagenlogische Erfüllbarkeitsproblem keinen Polynomialzeitalgorithmus.
- Man vermutet sogar, dass es eine Konstante  $c > 1$  gibt, so dass jeder Algorithmus für 3-SAT eine worst-case Laufzeit von  $\Omega(c^n)$  hat. Diese Vermutung ist unter dem Namen „*Exponential Time Hypothesis*“ (*ETH*) bekannt.
- Der im Worst-Case beste derzeit bekannte Algorithmus für 3-SAT hat eine Laufzeit von etwa  $O(1.4^n)$ .

Folie 140

## Der Wahrheitstafelalgorithmus

Sind eine aussagenlogische Formel und eine Interpretation der in ihr vorkommenden Aussagensymbole gegeben, so kann man die Formel „bottom-up“ entlang ihres Syntaxbaums auswerten. Dies führt zu folgendem Lemma.

**Lemma 2.62.** *Es gibt einen Linearzeitalgorithmus, der bei Eingabe einer Formel  $\varphi(A_1, \dots, A_n) \in \text{AL}$  und eines Tupels  $(b_1, \dots, b_n) \in \{0, 1\}^n$  den Wert  $\varphi[b_1, \dots, b_n]$  berechnet.*

*Beweis:* Übung.

Der folgende Algorithmus löst das aussagenlogische Erfüllbarkeitsproblem.

### Wahrheitstafelalgorithmus

*Eingabe:* eine Formel  $\varphi \in \text{AL}$

1. Berechne die Wahrheitstafel für  $\varphi$ .
2. Falls in der letzten Spalte mindestens eine 1 auftaucht, gib „erfüllbar“ aus, sonst gib „unerfüllbar“ aus.

*Laufzeit:*  $O(m \cdot 2^n)$  (sogar im „Best-Case“)

Folie 141

## Der Resolutionsalgorithmus

Der Resolutionsalgorithmus probiert einfach alle möglichen Resolutionsableitungen durch und testet so, ob es eine Resolutionswiderlegung gibt (d.h. die Klauselmenge unerfüllbar ist).

### Resolutionsalgorithmus

*Eingabe:* eine endliche Klauselmenge  $\Gamma$  (entspricht einer KNF-Formel)

1. Wiederhole, bis keine neuen Klauseln mehr generiert werden:  
Füge alle Resolventen aller Klauseln aus  $\Gamma$  zu  $\Gamma$  hinzu.
2. Falls  $\emptyset \in \Gamma$ , gib „unerfüllbar“ aus, sonst gib „erfüllbar“ aus.

*Laufzeit:*

$2^{O(n)}$  (weil es bei  $n$  Aussagensymbolen  $4^n$  verschiedene Klauseln gibt).

Folie 142

## Der Davis-Putnam-Logemann-Loveland Algorithmus

Der DPLL-Algorithmus ist ein in der Praxis sehr erfolgreicher Algorithmus, der die Wahrheitstafelmethode mit Resolution kombiniert. Ähnlich wie bei dem Wahrheitstafelalgorithmus durchsucht der DPLL-Algorithmus systematisch den Raum aller möglichen Interpretationen und testet, ob diese die gegebene Klauselmenge erfüllen. Resolution wird dabei dazu verwendet, die Suche geschickt zu steuern und Dinge, die während der Suche bereits über die Klauselmenge „gelernt“ wurden, weiterzuverwenden. Der DPLL-Algorithmus ist die Basis moderner SAT-Solver, die Klauselmengen, die aus Millionen von Klauseln und Hunderttausenden von Aussagensymbolen bestehen, auf Erfüllbarkeit testen können.

Folie 143

### DPLL-Algorithmus

*Eingabe:* eine endliche Klauselmenge  $\Gamma$  (entspricht einer KNF-Formel)

1. Vereinfache  $\Gamma$ . *% Details dazu: siehe nächste Folie*
2. Falls  $\Gamma = \emptyset$ , gib „erfüllbar“ aus.
3. Falls  $\emptyset \in \Gamma$ , gib „unerfüllbar“ aus.
4. Wähle ein Literal  $\lambda$ .
5. *% probiere aus, ob  $\Gamma$  ein Modell hat, bei dem das Literal  $\lambda$  erfüllt wird:*  
Löse rekursiv  $\Gamma \cup \{\{\lambda\}\}$ . Falls dies erfüllbar ist, gib „erfüllbar“ aus.
6. *% probiere aus, ob  $\Gamma$  ein Modell hat, bei dem das Literal  $\bar{\lambda}$  erfüllt wird:*  
Löse rekursiv  $\Gamma \cup \{\{\bar{\lambda}\}\}$ . Falls dies erfüllbar ist, gib „erfüllbar“ aus.  
Sonst gib „unerfüllbar“ aus.

Folie 144

### Vereinfachungsheuristiken, die in Schritt 1. angewendet werden:

- *Unit Propagation:*  
Für alle „Einerklauseln“  $\{\lambda\} \in \Gamma$  (wobei  $\lambda$  ein Literal ist), bilde alle Resolventen von  $\{\lambda\}$  mit anderen Klauseln und streiche anschließend alle Klauseln, die  $\lambda$  enthalten. Wiederhole dies, so lange es Einerklauseln gibt.

*Präzise:*

Für jede „Einerklausel“  $\{\lambda\} \in \Gamma$  tue Folgendes:

1. Ersetze jede Klausel  $\gamma \in \Gamma$  durch die Klausel  $\gamma \setminus \{\bar{\lambda}\}$ .
2. Entferne aus  $\Gamma$  jede Klausel, die das Literal  $\lambda$  enthält.

Wiederhole dies, so lange es in  $\Gamma$  Einerklauseln gibt.

- *Pure Literal Rule:*

Literale  $\lambda$ , deren Negat  $\bar{\lambda}$  nirgendwo in der Klauselmenge auftaucht, können auf 1 gesetzt werden. Alle Klauseln, die ein solches Literal enthalten, sind dann wahr und können gestrichen werden.

Wiederhole dies, so lange es Literale gibt, deren Negat nirgendwo in der Klauselmenge auftaucht.

- Streiche Klauseln, die Obermengen von anderen Klauseln sind (dies ist allerdings ineffizient und wird in der Praxis zumeist weggelassen).

Man sieht leicht, dass das Anwenden dieser Vereinfachungsheuristiken die Klauselmenge  $\Gamma$  in eine erfüllbarkeitsäquivalente Klauselmenge transformiert. Hieraus folgt leicht, dass der DPLL-Algorithmus stets die korrekte Antwort gibt (d.h., er terminiert immer, und er gibt genau dann „erfüllbar“ aus, wenn die eingegebene Klauselmenge  $\Gamma$  erfüllbar ist).

*Laufzeit des DPLL-Algorithmus:*

$O(m \cdot 2^n)$  im Worst-Case; in der Praxis aber häufig sehr effizient.

Folie 145

**Beispiel 2.63.** Sei  $\Gamma :=$

$$\begin{aligned} & \{ \{X_1, \neg X_5, \neg X_6, X_7\}, \{\neg X_1, X_2, \neg X_5\}, \{\neg X_1, \neg X_2, \neg X_3, \neg X_5, \neg X_6\}, \\ & \{X_1, X_2, \neg X_4, X_7\}, \{\neg X_4, \neg X_6, \neg X_7\}, \{X_3, \neg X_5, X_7\}, \\ & \{X_3, \neg X_4, \neg X_5\}, \{X_5, \neg X_6\}, \{X_5, X_4, \neg X_8\}, \\ & \{X_1, X_3, X_5, X_6, X_7\}, \{\neg X_7, X_8\}, \{\neg X_6, \neg X_7, \neg X_8\} \} \end{aligned}$$

*Ein Lauf des DPLL-Algorithmus:*

(1) Keine Vereinfachung möglich.  $\Gamma \neq \emptyset$ .  $\emptyset \notin \Gamma$ .

Wähle das Literal<sup>2</sup>  $\lambda := X_6$  und wende den Algorithmus rekursiv auf  $\Gamma \cup \{\{X_6\}\}$  an.

---

<sup>2</sup>Welches Literal genau gewählt wird, ist im Algorithmus nicht festgelegt. Wir wählen ein beliebiges Literal aus, das in  $\Gamma$  vorkommt.

(2) Unit Propagation mit  $\{X_6\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{X_1, \neg X_5, X_7\}, \{\neg X_1, X_2, \neg X_5\}, \{\neg X_1, \neg X_2, \neg X_3, \neg X_5\}, \\ & \{X_1, X_2, \neg X_4, X_7\}, \{\neg X_4, \neg X_7\}, \{X_3, \neg X_5, X_7\}, \\ & \{X_3, \neg X_4, \neg X_5\}, \{X_5\}, \{X_5, X_4, \neg X_8\}, \\ & \{\cancel{X_1, X_3, X_5, X_6, X_7}\}, \{\neg X_7, X_8\}, \{\neg X_7, \neg X_8\}, \{\cancel{X_6}\} \end{aligned}$$

(3) Unit Propagation mit  $\{X_5\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{X_1, X_7\}, \{\neg X_1, X_2\}, \{\neg X_1, \neg X_2, \neg X_3\}, \\ & \{X_1, X_2, \neg X_4, X_7\}, \{\neg X_4, \neg X_7\}, \{X_3, X_7\}, \\ & \{X_3, \neg X_4\}, \{\cancel{X_5}\}, \{\cancel{X_5, X_4, \neg X_8}\}, \\ & \{\neg X_7, X_8\}, \{\neg X_7, \neg X_8\} \} \end{aligned}$$

(4) Pure Literal Rule mit  $\neg X_4$  liefert die Klauselmenge

$$\begin{aligned} \Gamma' := & \{ \{X_1, X_7\}, \{\neg X_1, X_2\}, \{\neg X_1, \neg X_2, \neg X_3\}, \\ & \{\cancel{X_1, X_2, \neg X_4, X_7}\}, \{\cancel{\neg X_4, \neg X_7}\}, \{X_3, X_7\}, \\ & \{\cancel{X_3, \neg X_4}\}, \\ & \{\neg X_7, X_8\}, \{\neg X_7, \neg X_8\} \} \end{aligned}$$

(5) Keine weitere Vereinfachung von  $\Gamma'$  möglich.  $\Gamma' \neq \emptyset$ .  $\emptyset \notin \Gamma'$ .  
Wähle das Literal<sup>3</sup>  $\lambda := X_7$  und wende den Algorithmus rekursiv auf  $\Gamma' \cup \{\{X_7\}\}$  an.

(6) Unit Propagation mit  $\{X_7\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{\cancel{X_1, X_7}\}, \{\neg X_1, X_2\}, \{\neg X_1, \neg X_2, \neg X_3\}, \\ & \{\cancel{X_3, X_7}\}, \\ & \{X_8\}, \{\neg X_8\}, \{\cancel{X_7}\} \} \end{aligned}$$

(7) Unit Propagation mit  $\{X_8\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{\neg X_1, X_2\}, \{\neg X_1, \neg X_2, \neg X_3\}, \\ & \{\cancel{X_8}\}, \emptyset \} \end{aligned}$$

Jetzt ist  $\emptyset$  in der Klauselmenge enthalten — d.h. die Klauselmenge ist nicht erfüllbar. Daher:

---

<sup>3</sup>Welches Literal genau gewählt wird, ist im Algorithmus nicht festgelegt. Wir wählen ein beliebiges Literal aus, das in der Klauselmenge vorkommt.

(8) Backtracking, zurück zu Schritt (5):  
Wende den Algorithmus auf  $\Gamma' \cup \{\{\neg X_7\}\}$  an.

(9) Unit Propagation mit  $\{\neg X_7\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{X_1\}, \{\neg X_1, X_2\}, \{\neg X_1, \neg X_2, \neg X_3\}, \\ & \quad \{X_3\}, \\ & \quad \{\cancel{\neg X_7, X_8}\}, \{\cancel{\neg X_7, \neg X_8}\}, \{\cancel{\neg X_7}\} \}. \end{aligned}$$

Danach führt Unit Propagation mit  $\{X_1\}$  zu

$$\{ \{\cancel{X_1}\}, \{X_2\}, \{\neg X_2, \neg X_3\}, \{X_3\} \}.$$

Dann führt Unit Propagation mit  $\{X_2\}$  zu

$$\{ \{\cancel{X_2}\}, \{\neg X_3\}, \{X_3\} \},$$

und Unit Propagation mit  $\{\neg X_3\}$  führt zu

$$\{ \{\cancel{\neg X_3}\}, \emptyset \}.$$

Jetzt ist  $\emptyset$  in der Klauselmenge enthalten — d.h. die Klauselmenge ist nicht erfüllbar. Daher:

(10) Backtracking, zurück zu Schritt (1):  
Wende den Algorithmus auf  $\Gamma \cup \{\{\neg X_6\}\}$  an.

(11) Unit Propagation mit  $\{\neg X_6\}$  liefert die Klauselmenge

$$\begin{aligned} & \{ \{\cancel{X_1, \neg X_5, \neg X_6, X_7}\}, \{\neg X_1, X_2, \neg X_5\}, \{\cancel{\neg X_1, \neg X_2, \neg X_3, \neg X_5, \neg X_6}\}, \\ & \quad \{X_1, X_2, \neg X_4, X_7\}, \{\cancel{\neg X_4, \neg X_6, \neg X_7}\}, \{X_3, \neg X_5, X_7\}, \\ & \quad \{X_3, \neg X_4, \neg X_5\}, \{\cancel{X_5, \neg X_6}\}, \{X_5, X_4, \neg X_8\}, \\ & \quad \{X_1, X_3, X_5, X_7\}, \{\neg X_7, X_8\}, \{\cancel{\neg X_6, \neg X_7, \neg X_8}\}, \{\cancel{\neg X_6}\} \} \end{aligned}$$

Etwas übersichtlicher aufgeschrieben, also die Klauselmenge

$$\begin{aligned} & \{ \{\neg X_1, X_2, \neg X_5\}, \\ & \quad \{X_1, X_2, \neg X_4, X_7\}, \{X_3, \neg X_5, X_7\}, \\ & \quad \{X_3, \neg X_4, \neg X_5\}, \{X_5, X_4, \neg X_8\}, \\ & \quad \{X_1, X_3, X_5, X_7\}, \{\neg X_7, X_8\} \} \end{aligned}$$



(12) Pure Literal Rule mit  $X_2$  und  $X_3$  liefert die Klauselmenge

$$\left\{ \overline{\{\neg X_1, X_2, \neg X_5\}}, \overline{\{X_1, X_2, \neg X_4, X_7\}}, \overline{\{X_3, \neg X_5, X_7\}}, \overline{\{X_3, \neg X_4, \neg X_5\}}, \{X_5, X_4, \neg X_8\}, \overline{\{X_1, X_3, X_5, X_7\}}, \{\neg X_7, X_8\} \right\},$$

etwas übersichtlicher aufgeschrieben also die Klauselmenge

$$\left\{ \{X_5, X_4, \neg X_8\}, \{\neg X_7, X_8\} \right\}.$$

(13) Pure Literal Rule mit  $X_5$  und  $\neg X_7$  liefert die Klauselmenge

$$\Gamma'' := \left\{ \overline{\{X_5, X_4, \neg X_8\}}, \overline{\{\neg X_7, X_8\}} \right\},$$

d.h.  $\Gamma''$  ist die *leere* Klauselmenge  $\emptyset$ .

(14) Also wird „erfüllbar“ ausgegeben.

## 2.8 Hornformeln

Folie 146

### Hornklauseln und Hornformeln

Hornformeln sind spezielle aussagenlogische Formeln, die die Basis der logischen Programmierung bilden, und für die das Erfüllbarkeitsproblem effizient gelöst werden kann.

**Definition 2.64.** Eine *Hornklausel* ist eine disjunktive Klausel, in der höchstens ein positives Literal vorkommt.

Eine *Hornformel* ist eine Konjunktion endlich vieler Hornklauseln.

*Beispiele.*

- $\{\neg X, \neg Y, \neg Z\}$  (bzw.  $\neg X \vee \neg Y \vee \neg Z$ ) ist eine Hornklausel.
- $\{\neg X, \neg Y, Z\}$  (bzw.  $\neg X \vee \neg Y \vee Z$ ) ist eine Hornklausel.
- $\{\neg X, Y, Z\}$  (bzw.  $\neg X \vee Y \vee Z$ ) ist keine Hornklausel.
- $\{X\}$  (bzw.  $X$ ) ist eine Hornklausel.
- $\emptyset$  ist eine Hornklausel.
- $(X \vee \neg Y) \wedge (\neg Z \vee \neg X \vee \neg Y) \wedge Y$  ist eine Hornformel.

Folie 147

## Hornklauseln als Implikationen

- Eine Hornklausel der Form  $\{\neg X_1, \dots, \neg X_{n-1}, X_n\}$  (bzw.  $\neg X_1 \vee \dots \vee \neg X_{n-1} \vee X_n$ ) ist äquivalent zur Formel

$$(X_1 \wedge \dots \wedge X_{n-1}) \rightarrow X_n.$$

Solche Klauseln werden auch „Regeln“ (oder „Prozedurklauseln“) genannt.

- Eine Hornklausel der Form  $\{\neg X_1, \dots, \neg X_{n-1}\}$  ist äquivalent zur Formel

$$(X_1 \wedge \dots \wedge X_{n-1}) \rightarrow \mathbf{0}.$$

Solche Klauseln werden auch „Zielklauseln“ (oder „Frageklauseln“) genannt.

- Eine Hornklausel der Form  $\{X_1\}$  ist äquivalent zur Formel

$$\mathbf{1} \rightarrow X_1.$$

Solche Klauseln werden auch „Tatsachenklausel“ genannt.

- Die leere (Horn-)Klausel  $\emptyset$  ist unerfüllbar und daher äquivalent zur Formel

$$\mathbf{1} \rightarrow \mathbf{0}.$$

Folie 148

## Der Streichungsalgorithmus

Der folgende Algorithmus löst das Erfüllbarkeitsproblem für Hornformeln in Polynomialzeit.

Wir geben zunächst den Algorithmus an, betrachten dann Beispielläufe davon, analysieren die Laufzeit und zeigen danach, dass der Algorithmus korrekt ist, d.h. stets die richtige Antwort gibt.

Folie 149

### Streichungsalgorithmus

*Eingabe:* eine endliche Menge  $\Gamma$  von Hornklauseln

1. Wiederhole:
2. Falls  $\emptyset \in \Gamma$ , so halte mit Ausgabe „unerfüllbar“.

3. Falls  $\Gamma$  keine Tatsachenklausel (d.h. Klausel  $\{X\}$  mit  $X \in \text{AS}$ ) enthält, so halte mit Ausgabe „erfüllbar“.
 

*%  $\Gamma$  wird erfüllt, indem jedes Aussagensymbol mit 0 belegt wird*
4. Wähle eine Tatsachenklausel  $\{X\} \in \Gamma$ .
 

*% Idee: Um  $\Gamma$  zu erfüllen, muss  $X$  mit dem Wert 1 belegt werden*
5. Streiche  $\neg X$  aus allen Klauseln  $\delta \in \Gamma$ , die das Literal  $\neg X$  enthalten.
 

*% Wenn  $X$  den Wert 1 hat, trägt  $\neg X$  nichts zum Erfüllen einer Klausel bei*
6. Streiche aus  $\Gamma$  alle Klauseln  $\delta \in \Gamma$ , die das Literal  $X$  enthalten (d.h. entferne aus  $\Gamma$  alle  $\delta \in \Gamma$ , für die gilt:  $X \in \delta$ ).
 

*% Wenn  $X$  den Wert 1 hat, sind solche Klauseln erfüllt*

Folie 150

**Beispiele 2.65.** Wir wenden den Streichungsalgorithmus auf die beiden folgenden Mengen von Hornklauseln an.

$$(a) \Gamma_a := \{ S \rightarrow \mathbf{0}, (P \wedge Q) \rightarrow R, (S \wedge R) \rightarrow \mathbf{0}, (U \wedge T \wedge Q) \rightarrow P, \\ (U \wedge T) \rightarrow Q, \mathbf{1} \rightarrow U, \mathbf{1} \rightarrow T \}$$

$$(b) \Gamma_b := \{ (Q \wedge P) \rightarrow T, (U \wedge T \wedge Q) \rightarrow R, (U \wedge T) \rightarrow Q, \\ \mathbf{1} \rightarrow U, R \rightarrow \mathbf{0}, \mathbf{1} \rightarrow T \}$$

(a): Beispiel-Lauf des Streichungsalgorithmus bei Eingabe von  $\Gamma_a$ :

Beachte, dass  $\Gamma_a$  der folgenden Klauselmenge entspricht:

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg U, \neg T, \neg Q, P\}, \\ \{\neg U, \neg T, Q\}, \{U\}, \{T\} \}$$

1. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{U\} \in \Gamma$ , streiche  $\neg U$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $U$  enthalten:

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg U, \neg T, \neg Q, P\}, \\ \{\neg U, \neg T, Q\}, \{\cancel{U}\}, \{T\} \},$$

d.h.

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg T, \neg Q, P\}, \\ \{\neg T, Q\}, \{T\} \}.$$

2. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{T\} \in \Gamma$ , streiche  $\neg T$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $T$  enthalten:

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg T, \neg Q, P\}, \\ \{\neg T, Q\}, \{\cancel{T}\} \},$$

d.h.

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg Q, P\}, \\ \{Q\} \}.$$

3. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{Q\} \in \Gamma$ , streiche  $\neg Q$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $Q$  enthalten:

$$\Gamma = \{ \{\neg S\}, \{\neg P, \neg Q, R\}, \{\neg S, \neg R\}, \{\neg Q, P\}, \\ \{\cancel{Q}\} \},$$

d.h.

$$\Gamma = \{ \{\neg S\}, \{\neg P, R\}, \{\neg S, \neg R\}, \{P\} \}.$$

4. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{P\} \in \Gamma$ , streiche  $\neg P$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $P$  enthalten:

$$\Gamma = \{ \{\neg S\}, \{\neg P, R\}, \{\neg S, \neg R\}, \{\cancel{P}\} \},$$

d.h.

$$\Gamma = \{ \{\neg S\}, \{R\}, \{\neg S, \neg R\} \}.$$

5. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{R\} \in \Gamma$ , streiche  $\neg R$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $R$  enthalten:

$$\Gamma = \{ \{\neg S\}, \{\cancel{R}\}, \{\neg S, \neg R\} \}$$

d.h.

$$\Gamma = \{ \{\neg S\}, \{\neg S\} \}$$

6. Schleifendurchlauf:

$\emptyset \notin \Gamma$ .  $\Gamma$  enthält keine Tatsachenklausel.

D.h.: Halte mit Ausgabe „erfüllbar“.

(b) Beispiel-Lauf des Streichungsalgorithmus bei Eingabe von  $\Gamma_b$ :

Beachte, dass  $\Gamma_b$  der folgenden Klauselmenge entspricht:

$$\Gamma = \{ \{ \neg Q, \neg P, T \}, \{ \neg U, \neg T, \neg Q, R \}, \{ \neg U, \neg T, Q \}, \\ \{ U \}, \{ \neg R \}, \{ T \} \}$$

1. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{ U \} \in \Gamma$ , streiche  $\neg U$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $U$  enthalten:

$$\Gamma = \{ \{ \neg Q, \neg P, T \}, \{ \neg \cancel{U}, \neg T, \neg Q, R \}, \{ \neg \cancel{U}, \neg T, Q \}, \\ \cancel{\{ U \}}, \{ \neg R \}, \{ T \} \},$$

d.h.

$$\Gamma = \{ \{ \neg Q, \neg P, T \}, \{ \neg T, \neg Q, R \}, \{ \neg T, Q \}, \{ \neg R \}, \{ T \} \}.$$

2. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{ T \} \in \Gamma$ , streiche  $\neg T$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $T$  enthalten:

$$\Gamma = \{ \cancel{\{ \neg Q, \neg P, T \}}, \{ \neg \cancel{T}, \neg Q, R \}, \{ \neg \cancel{T}, Q \}, \{ \neg R \}, \cancel{\{ T \}} \},$$

d.h.

$$\Gamma = \{ \{ \neg Q, R \}, \{ Q \}, \{ \neg R \} \}.$$

3. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{ Q \} \in \Gamma$ , streiche  $\neg Q$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $Q$  enthalten:

$$\Gamma = \{ \{ \neg \cancel{Q}, R \}, \cancel{\{ Q \}}, \{ \neg R \} \},$$

d.h.

$$\Gamma = \{ \{ R \}, \{ \neg R \} \}.$$

4. Schleifendurchlauf:

$\emptyset \notin \Gamma$ . Wähle  $\{ R \} \in \Gamma$ , streiche  $\neg R$  aus allen Klauseln in  $\Gamma$ , und streiche alle Klauseln, die  $R$  enthalten:

$$\Gamma = \{ \cancel{\{ R \}}, \{ \neg \cancel{R} \} \},$$

d.h.

$$\Gamma = \{ \emptyset \}.$$

5. Schleifendurchlauf:

$\emptyset \in \Gamma$ . D.h.: Halte mit Ausgabe „unerfüllbar“.

## Laufzeit des Streichungsalgorithmus

Man sieht leicht, dass in jedem Schleifendurchlauf die Anzahl der Klauseln in  $\Gamma$  kleiner wird. Daher terminiert der Algorithmus nach maximal  $m$  Schleifendurchläufen, wobei  $m$  die Anzahl der Klauseln in der Eingabemenge  $\Gamma$  ist.

In jedem einzelnen Schleifendurchlauf betrachtet der Algorithmus alle Klauseln der aktuellen Klauselmenge und führt dabei  $O(n)$  Schritte durch, wobei  $n = \|\Gamma\|$  die Größe der Klauselmenge ist.

Insgesamt terminiert der Streichungsalgorithmus also nach  $O(m \cdot n)$  Schritten, d.h. in Zeit polynomiell in der Größe von  $\Gamma$ .

Insgesamt erhalten wir also folgenden Satz:

**Satz 2.66.** *Die Laufzeit des Streichungsalgorithmus ist  $O(m \cdot n)$ , wobei  $m = |\Gamma|$  die Anzahl der Hornklauseln in der eingegebenen Menge  $\Gamma$  und  $n = \|\Gamma\|$  die Größe von  $\Gamma$  ist.*

**Bemerkung.** Eine Variante des Streichungsalgorithmus läuft sogar in Linearzeit, d.h. in Zeit  $O(n)$ .

Um nachzuweisen, dass der Streichungsalgorithmus stets die korrekte Antwort gibt, nutzen wir das folgende Lemma.

Folie 152

## Der Streichungsalgorithmus und Resolution

**Lemma 2.67.** *Sei  $\Gamma_0$  eine endliche Menge von Hornklauseln und  $\delta$  eine Klausel, die zu irgendeinem Zeitpunkt während des Laufs des Streichungsalgorithmus bei Eingabe  $\Gamma_0$  in der vom Algorithmus gespeicherten Menge  $\Gamma$  liegt. Dann gilt:  $\Gamma_0 \vdash_R \delta$ .*

*Beweis.*

Wir betrachten einen Lauf des Streichungsalgorithmus bei Eingabe  $\Gamma_0$ . Sei  $\ell$  die Anzahl der Durchläufe der Schleife, die der Algorithmus durchführt. Für jedes  $i \in \{1, \dots, \ell\}$  sei  $\Gamma_i$  die Menge  $\Gamma$  am Ende des  $i$ -ten Durchlaufs der Schleife. Per Induktion nach  $i$  zeigen wir, dass für alle  $i \in \{0, \dots, \ell\}$  gilt:

Für jedes  $\delta \in \Gamma_i$  ist  $\Gamma_0 \vdash_R \delta$ .

*Induktionsanfang:*  $i = 0$ :

Offensichtlicherweise gilt für alle  $\delta \in \Gamma_0$ , dass  $\Gamma_0 \vdash_R \delta$ .

*Induktionsschritt:*  $i \rightarrow i+1$ : Sei  $\delta \in \Gamma_{i+1}$ .

Falls  $\delta \in \Gamma_i$ , so gilt  $\Gamma_0 \vdash_R \delta$  gemäß Induktionsannahme.

Falls  $\delta \notin \Gamma_i$ , so wird  $\delta$  beim  $i+1$ -ten Schleifendurchlauf in Zeile 5 neu erzeugt. Also gibt es ein Aussagensymbol  $X$  mit  $\{X\} \in \Gamma_i$  und eine Klausel  $\delta' \in \Gamma_i$ , so dass  $\neg X \in \delta'$  und  $\delta = \delta' \setminus \{\neg X\}$ . Dann ist  $\delta$  eine Resolvente von  $\delta'$  und  $\{X\}$ . Gemäß Induktionsannahme gilt  $\Gamma_0 \vdash_R \delta'$  und  $\Gamma_0 \vdash_R \{X\}$ . Also gilt auch  $\Gamma_0 \vdash_R \delta$ .  $\square$

Folie 153

## Korrektheit des Streichungsalgorithmus

**Satz 2.68.** *Der Streichungsalgorithmus ist korrekt.*

*Das heißt, bei Eingabe einer endlichen Menge  $\Gamma_0$  von Hornklauseln hält der Algorithmus mit Ausgabe „erfüllbar“, falls  $\Gamma_0$  erfüllbar ist, und mit Ausgabe „nicht erfüllbar“, falls  $\Gamma_0$  unerfüllbar ist.*

*Beweis.*

Wir betrachten einen Lauf des Streichungsalgorithmus bei Eingabe  $\Gamma_0$ .

Sei  $\ell$  die Anzahl der Durchläufe der Schleife, die der Algorithmus durchführt. Für  $i \in \{1, \dots, \ell\}$  sei  $\Gamma_i$  die Menge  $\Gamma$  am Ende des  $i$ -ten Durchlaufs der Schleife. Für jedes  $i$  mit  $1 \leq i < \ell$  sei  $X_i$  das Aussagensymbol, so dass im  $i$ -ten Durchlauf in Zeile 4 die Tatsachenklausel  $\{X_i\} \in \Gamma_{i-1}$  ausgewählt wird.

*Fall 1:* Der Algorithmus hält beim  $\ell$ -ten Durchlauf der Schleife in Zeile 2. Dann gilt  $\emptyset \in \Gamma_{\ell-1}$  und daher gilt nach Lemma 2.67, dass  $\Gamma_0 \vdash_R \emptyset$ . Also besitzt  $\Gamma_0$  eine Resolutionswiderlegung und ist daher gemäß Satz 2.59 unerfüllbar.

*Fall 2:* Der Algorithmus hält beim  $\ell$ -ten Durchlauf der Schleife in Zeile 3. Dann enthält jede Klausel von  $\Gamma_{\ell-1}$  mindestens ein negatives Literal (denn  $\Gamma_0$  ist laut Voraussetzung eine Menge von Hornklauseln, und der Algorithmus geht so vor, dass auch jedes  $\Gamma_i$  eine Menge von Hornklauseln ist). Also erfüllt die „Nullinterpretation“  $\mathcal{I}_0$  mit  $\mathcal{I}_0(Y) := 0$  für alle  $Y \in \text{AS}$  die Klauselmenge  $\Gamma_{\ell-1}$ . Wir definieren die Interpretation  $\mathcal{I}$  durch

$$\mathcal{I}(X_1) = \mathcal{I}(X_2) = \dots = \mathcal{I}(X_{\ell-1}) = 1, \quad \text{und}$$

$$\mathcal{I}(Z) = 0 \quad \text{für alle } Z \in \text{AS} \setminus \{X_1, \dots, X_{\ell-1}\}.$$

Per Induktion nach  $i$  zeigen wir, dass für alle  $i \in \{\ell-1, \ell-2, \dots, 0\}$  gilt:

$$\mathcal{I} \models \Gamma_i.$$

Für  $i = 0$  erhalten wir dann, dass  $\mathcal{I} \models \Gamma_0$ ; insbesondere ist  $\Gamma_0$  also erfüllbar.

*Induktionsanfang:*  $i = \ell-1$ : Wir wissen, dass  $\mathcal{I}_0 \models \Gamma_{\ell-1}$ . Außerdem kommt gemäß der Konstruktion des Streichungsalgorithmus in  $\Gamma_{\ell-1}$  keins der Symbole  $X_1, \dots, X_{\ell-1}$  vor. Auf allen anderen Aussagensymbolen stimmen  $\mathcal{I}$  und  $\mathcal{I}_0$  überein. Gemäß Koinzidenzlemma gilt also  $\mathcal{I} \models \Gamma_{\ell-1}$ .

*Induktionsschritt:*  $i \rightarrow i-1$ : Gemäß Induktionsannahme gilt  $\mathcal{I} \models \Gamma_i$ . Ziel ist, zu zeigen, dass auch gilt:  $\mathcal{I} \models \Gamma_{i-1}$ . Sei dazu  $\delta$  eine beliebige Klausel aus  $\Gamma_{i-1}$ .

*Fall 1:*  $\delta \in \Gamma_i$ .

Dann gilt  $\mathcal{I} \models \delta$  gemäß Induktionsannahme.

*Fall 2:*  $\delta \in \Gamma_{i-1} \setminus \Gamma_i$ .

*Fall 2.1:*  $\delta$  ist im  $i$ -ten Schleifendurchlauf gemäß Zeile 5 modifiziert worden, d.h.  $\delta = \delta' \cup \{\neg X_i\}$  für ein  $\delta' \in \Gamma_i$ . Gemäß Induktionsannahme gilt  $\mathcal{I} \models \delta'$ , und daher gilt auch  $\mathcal{I} \models \delta$ .

*Fall 2.2:*  $\delta$  ist im  $i$ -ten Schleifendurchlauf gemäß Zeile 6 aus der Klauselmenge entfernt worden, d.h.  $X_i \in \delta$ . Wegen  $\mathcal{I}(X_i) = 1$  gilt dann  $\mathcal{I} \models \delta$ .

□



## *Kapitel 3*

# Logik erster Stufe

### 3.1 Strukturen

Folie 154

#### Strukturen

Wir führen einen allgemeinen Strukturbegriff ein, der es uns erlaubt:

- mathematische Strukturen wie Gruppen, Körper, Vektorräume, Graphen, etc.
- und die gängigen Modelle der Informatik wie Transitionssysteme, endliche Automaten, relationale Datenbanken, Schaltkreise, etc.

zu beschreiben.

Folie 155

#### Signaturen

**Definition 3.1.** Eine *Signatur* (auch *Vokabular* oder *Symbolmenge*) ist eine Menge  $\sigma$  von *Relations-*, *Funktions-* und/oder *Konstantensymbolen*.

Jedes Relationsymbol  $R \in \sigma$  und jedes Funktionssymbol  $f \in \sigma$  hat eine *Stelligkeit* (bzw. *Arität*, engl. *arity*)

$$\text{ar}(R) \in \mathbb{N} \setminus \{0\} \quad \text{bzw.} \quad \text{ar}(f) \in \mathbb{N} \setminus \{0\}.$$

Folie 156

## Notation

- In diesem Kapitel bezeichnet der griechische Buchstabe  $\sigma$  (in Worten: sigma) immer eine Signatur.
- Für Relationssymbole verwenden wir normalerweise Großbuchstaben wie  $R, P, Q, E$ , für Funktionssymbole verwenden wir meistens Kleinbuchstaben wie  $f, g, h$  und für Konstantensymbole Kleinbuchstaben wie  $c, d$ .
- Gelegentlich verwenden wir als Relations- und Funktionssymbole auch Zeichen wie  $\leq$  (2-stelliges Relationssymbol) und  $+, \cdot$  (2-stellige Funktionssymbole), und wir verwenden  $\underline{0}, \underline{1}$  als Konstantensymbole.
- Die Stelligkeit eines Relations- oder Funktionssymbols deuten wir häufig an, indem wir sie mit Schrägstrich hinter das Symbol schreiben.

*Beispiel.* Die Notation  $R/2$  deutet an, dass  $R$  ein 2-stelliges Relationssymbol ist.

Folie 157

## Strukturen

**Definition 3.2.** Eine  $\sigma$ -Struktur  $\mathcal{A}$  besteht aus folgenden Komponenten:

- einer nicht-leeren Menge  $A$ , dem *Universum* von  $\mathcal{A}$  (auch: *Träger*, engl. universe, domain),
- für jedes Relationssymbol  $R \in \sigma$  und für  $k := \text{ar}(R)$  gibt es eine  $k$ -stellige Relation  $R^{\mathcal{A}} \subseteq A^k$ ,
- für jedes Funktionssymbol  $f \in \sigma$  und für  $k := \text{ar}(f)$  gibt es eine  $k$ -stellige Funktion  $f^{\mathcal{A}} : A^k \rightarrow A$ , und
- für jedes Konstantensymbol  $c \in \sigma$  gibt es ein Element  $c^{\mathcal{A}} \in A$ .

Folie 158

## Notation.

- Wir beschreiben  $\sigma$ -Strukturen oft in Tupelschreibweise:  
 $\mathcal{A} = (A, (S^A)_{S \in \sigma})$ .  
 Falls  $\sigma = \{S_1, \dots, S_k\}$  endlich ist, schreiben wir auch  
 $\mathcal{A} = (A, S_1^A, \dots, S_k^A)$ .
- Wir bezeichnen  $\sigma$ -Strukturen meistens mit „kalligraphischen“  
 Buchstaben wie  $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{W}, \dots$ . Das Universum der Strukturen  
 bezeichnen wir dann durch die entsprechenden lateinischen  
 Großbuchstaben, also  $A, B, C, W, \dots$ .

Folie 159

## Mengen

Für die leere Signatur  $\sigma := \emptyset$  bestehen  $\sigma$ -Strukturen nur aus ihrem  
 Universum, sind also einfach (nicht-leere) Mengen.

Folie 160

## Graphen

In diesem Kapitel bezeichnet  $E$  immer ein zweistelliges Relationssymbol.

- Ein *gerichteter Graph* (kurz: *Digraph*)  $\mathcal{G} = (V^{\mathcal{G}}, E^{\mathcal{G}})$  mit  
 Knotenmenge  $V^{\mathcal{G}}$  und Kantenmenge  $E^{\mathcal{G}}$  ist eine  $\{E\}$ -Struktur. Das  
 Universum ist die Knotenmenge  $V^{\mathcal{G}}$ .
- Einen *ungerichteten Graphen*  $\mathcal{G} = (V^{\mathcal{G}}, E^{\mathcal{G}})$  mit Knotenmenge  $V^{\mathcal{G}}$  und  
 Kantenmenge  $E^{\mathcal{G}} \subseteq \{e \subseteq V^{\mathcal{G}} : |e| = 2\}$  repräsentieren wir durch eine  
 $\{E\}$ -Struktur  $\mathcal{A} = (A, E^{\mathcal{A}})$  mit Universum  $A = V^{\mathcal{G}}$  und Relation  
 $E^{\mathcal{A}} = \{(u, v) : \{u, v\} \in E^{\mathcal{G}}\}$ . Insbesondere ist  $E^{\mathcal{A}}$  *symmetrisch* und  
*irreflexiv* im Sinne der folgenden Definition.

Folie 161

## Eigenschaften zweistelliger Relationen

**Definition 3.3.** Sei  $\mathcal{A} = (A, R^{\mathcal{A}})$ , wobei  $R^{\mathcal{A}}$  eine zweistellige Relation über  
 der Menge  $A$  ist (d.h.  $(A, R^{\mathcal{A}})$  ist ein gerichteter Graph).

- (a)  $R^{\mathcal{A}}$  heißt *reflexiv*, wenn für alle  $a \in A$  gilt:  $(a, a) \in R^{\mathcal{A}}$ .  
 $R^{\mathcal{A}}$  heißt *irreflexiv*, wenn für alle  $a \in A$  gilt:  $(a, a) \notin R^{\mathcal{A}}$ .

(b)  $R^A$  heißt *symmetrisch*, wenn für alle  $a, b \in A$  gilt:

Wenn  $(a, b) \in R^A$ , dann ist auch  $(b, a) \in R^A$ .

$R^A$  heißt *antisymmetrisch*, wenn für alle  $a, b \in A$  mit  $a \neq b$  gilt:

Wenn  $(a, b) \in R^A$ , dann  $(b, a) \notin R^A$ .

(c)  $R^A$  heißt *transitiv*, wenn für alle  $a, b, c \in A$  gilt:

Wenn  $(a, b) \in R^A$  und  $(b, c) \in R^A$ , dann auch  $(a, c) \in R^A$ .

(d)  $R^A$  heißt *konnex*, wenn für alle  $a, b \in A$  gilt:

$(a, b) \in R^A$  oder  $(b, a) \in R^A$  oder  $a = b$ .

Folie 162

## Äquivalenzrelationen

Eine *Äquivalenzrelation* auf einer Menge  $A$  ist eine 2-stellige Relation über  $A$ , die *reflexiv*, *transitiv* und *symmetrisch* ist.

*Beispiele.*

- (a) *Gleichheit:* Für jede Menge  $M$  ist  $\{(m, m) : m \in M\}$  eine Äquivalenzrelation auf  $M$ .
- (b) *Gleichmächtigkeit:* Für jede endliche Menge  $M$  und deren Potenzmenge  $\mathcal{P}(M) = \{N : N \subseteq M\}$  gilt:  
 $\{(A, B) : A, B \subseteq M, |A| = |B|\}$  ist eine Äquivalenzrelation auf  $\mathcal{P}(M)$ .
- (c) *Logische Äquivalenz:* Die Relation  $\{(\varphi, \psi) : \varphi, \psi \in \mathbf{AL}, \varphi \equiv \psi\}$  ist eine Äquivalenzrelation auf der Menge  $\mathbf{AL}$  aller aussagenlogischen Formeln.

Folie 163

## Ordnungen

In diesem Kapitel bezeichnet  $\leq$  immer ein zweistelliges Relationssymbol. Für  $\leq$  verwenden wir Infixschreibweise, d.h., wir schreiben  $x \leq^A y$  statt  $(x, y) \in \leq^A$ .

- (a) Eine *Präordnung* ist eine  $\{\leq\}$ -Struktur  $\mathcal{A} = (A, \leq^A)$ , bei der  $\leq^A$  reflexiv und transitiv ist.
- (b) Eine *partielle Ordnung* (oder *Halbordnung*) ist eine Präordnung  $\mathcal{A}$ , bei der  $\leq^A$  antisymmetrisch ist.
- (c) Eine *lineare* (oder *totale*) *Ordnung* ist eine partielle Ordnung  $\mathcal{A}$ , bei der  $\leq^A$  konnex ist.

## Beispiele.

- (a) Die „*kleiner-gleich*“ Relation auf  $\mathbb{N}$  (oder  $\mathbb{Z}$  oder  $\mathbb{R}$ ) ist eine lineare Ordnung; die „*größer-gleich*“ auch.
- (b) Für jede Menge  $M$  ist die *Teilmengenrelation*  $\subseteq$  eine partielle Ordnung auf der Potenzmenge  $\mathcal{P}(M)$ ; aber keine lineare Ordnung, sofern  $M$  mindestens zwei Elemente besitzt (denn wenn  $a, b$  zwei verschiedene Elemente in  $M$  sind, gilt:  $\{a\} \not\subseteq \{b\}$  und  $\{b\} \not\subseteq \{a\}$  und  $\{a\} \neq \{b\}$ , und daher ist die Teilmengenrelation *nicht* konnex). Dasselbe gilt für die *Obermengenrelation*  $\supseteq$ .
- (c) Die *Folgerungsrelation für aussagenlogische Formeln*:  $\{(\varphi, \psi) : \varphi, \psi \in \text{AL}, \varphi \models \psi\}$  ist eine Präordnung auf der Menge  $\text{AL}$ , aber keine partielle Ordnung (denn beispielsweise gilt für  $\varphi := \mathbf{1}$  und  $\psi := \neg \mathbf{0}$ , dass  $\varphi \models \psi$  und  $\psi \models \varphi$  und  $\varphi \neq \psi$ , und daher ist die Folgerungsrelation *nicht* antisymmetrisch).

Folie 164

## Arithmetische Strukturen

$+$  und  $\cdot$  seien immer zweistellige Funktionssymbole, für die wir Infixschreibweise verwenden.  $\underline{0}$  und  $\underline{1}$  seien Konstantensymbole.

- Der *Körper der reellen Zahlen* ist die  $\{+, \cdot, \underline{0}, \underline{1}\}$ -Struktur  $\mathcal{A}_{\mathbb{R}}$ , so dass  $A_{\mathbb{R}} := \mathbb{R}$ ,  $+^{\mathcal{A}_{\mathbb{R}}}$  und  $\cdot^{\mathcal{A}_{\mathbb{R}}}$  sind die normale Addition bzw. Multiplikation auf  $\mathbb{R}$ , und  $\underline{0}^{\mathcal{A}_{\mathbb{R}}} := 0$ ,  $\underline{1}^{\mathcal{A}_{\mathbb{R}}} := 1$ .

- Der *Ring der ganzen Zahlen* ist die  $\{+, \cdot, \underline{0}, \underline{1}\}$ -Struktur  $\mathcal{A}_{\mathbb{Z}}$ , so dass  $A_{\mathbb{Z}} := \mathbb{Z}$ ,  $+^{\mathcal{A}_{\mathbb{Z}}}$  und  $\cdot^{\mathcal{A}_{\mathbb{Z}}}$  sind die normale Addition bzw. Multiplikation auf  $\mathbb{Z}$ , und  $\underline{0}^{\mathcal{A}_{\mathbb{Z}}} := 0$ ,  $\underline{1}^{\mathcal{A}_{\mathbb{Z}}} := 1$ .
- Das *Standardmodell der Arithmetik* ist die  $\{+, \cdot, \leq, \underline{0}, \underline{1}\}$ -Struktur  $\mathcal{A}_{\mathbb{N}}$ , so dass  $A_{\mathbb{N}} := \mathbb{N}$  ist; die Funktionen  $+^{\mathcal{A}_{\mathbb{N}}}$  und  $\cdot^{\mathcal{A}_{\mathbb{N}}}$  und die Relation  $\leq^{\mathcal{A}_{\mathbb{N}}}$  sind die normale Addition, Multiplikation bzw. Ordnung auf  $\mathbb{N}$ , und  $\underline{0}^{\mathcal{A}_{\mathbb{N}}} := 0$ ,  $\underline{1}^{\mathcal{A}_{\mathbb{N}}} := 1$ .
- Der *zweielementige Körper* ist die  $\{+, \cdot, \underline{0}, \underline{1}\}$ -Struktur  $\mathcal{F}_2$  mit Universum  $F_2 := \{0, 1\}$ , den Funktionen  $+^{\mathcal{F}_2}$  und  $\cdot^{\mathcal{F}_2}$  der Addition bzw. Multiplikation modulo 2, und  $\underline{0}^{\mathcal{F}_2} := 0$ ,  $\underline{1}^{\mathcal{F}_2} := 1$ .

Folie 165

## Wörter als Strukturen

Sei  $\Sigma$  ein endliches, nicht-leeres Alphabet. Für jedes  $a \in \Sigma$  sei  $P_a$  ein einstelliges Relationssymbol, und es sei

$$\sigma_{\Sigma} := \{\leq\} \cup \{P_a : a \in \Sigma\}.$$

Für jedes nicht-leere Wort  $w := w_1 \cdots w_n \in \Sigma^*$  mit  $w_1, \dots, w_n \in \Sigma$  sei  $\mathcal{A}_w$  die  $\sigma_{\Sigma}$ -Struktur

- mit Universum  $A_w := [n]$ , für die gilt:
- $\leq^{\mathcal{A}_w}$  ist die natürliche lineare Ordnung auf  $[n]$ , d.h.,  $\leq^{\mathcal{A}_w} = \{(i, j) : i, j \in \mathbb{N}, 1 \leq i \leq j \leq n\}$ ,
- Für jedes  $a \in \Sigma$  ist  $P_a^{\mathcal{A}_w} := \{i \in [n] : w_i = a\}$ .

**Beispiel.** Sei  $\Sigma := \{a, b, c\}$ .

Für  $w := abacaba$  ist  $\mathcal{A}_w$  die folgende  $\sigma_{\Sigma}$ -Struktur:

- $A_w = \{1, 2, 3, 4, 5, 6, 7\}$
- $\leq^{\mathcal{A}_w} = \{(i, j) : i, j \in \mathbb{N}, 1 \leq i \leq j \leq 7\}$
- $P_a^{\mathcal{A}_w} = \{1, 3, 5, 7\}$ ,  $P_b^{\mathcal{A}_w} = \{2, 6\}$ ,  $P_c^{\mathcal{A}_w} = \{4\}$ .

Folie 166

## Wortstrukturen

Eine *Wortstruktur über*  $\Sigma$  ist eine  $\sigma_\Sigma$ -Struktur  $\mathcal{A}$  für die gilt:

- das Universum  $A$  von  $\mathcal{A}$  ist endlich,
- $(A, \leq^{\mathcal{A}})$  ist eine lineare Ordnung,
- für jedes  $i \in A$  gibt es *genau ein*  $a \in \Sigma$ , so dass  $i \in P_a^{\mathcal{A}}$ .

**Beispiel 3.4.** Sei  $\Sigma := \{a, b, c\}$ . Die  $\sigma_\Sigma$ -Struktur  $\mathcal{B}$  mit

- Universum  $B = \{\diamond, \heartsuit, \spadesuit, \clubsuit\}$ ,
- linearer Ordnung  $\leq^{\mathcal{B}}$ , die besagt, dass  $\diamond < \heartsuit < \spadesuit < \clubsuit$  ist, d.h.  
 $\leq^{\mathcal{B}} = \{(\diamond, \diamond), (\diamond, \heartsuit), (\diamond, \spadesuit), (\diamond, \clubsuit), (\heartsuit, \heartsuit), (\heartsuit, \spadesuit), (\heartsuit, \clubsuit), (\spadesuit, \spadesuit), (\spadesuit, \clubsuit), (\clubsuit, \clubsuit)\}$ ,
- $P_a^{\mathcal{B}} = \{\diamond, \clubsuit\}$
- $P_b^{\mathcal{B}} = \{\heartsuit, \spadesuit\}$ ,
- $P_c^{\mathcal{B}} = \emptyset$ ,

ist eine Wortstruktur, die das Wort  $w = abba$  repräsentiert.

Folie 167

## Relationale Datenbanken

- *Relationale Datenbanken* bestehen aus endlich vielen endlichen Tabellen.
- Jede solche Tabelle lässt sich als Relation auffassen, die Zeilen der Tabelle entsprechen dabei den Tupeln in der Relation.
- Eine relationale Datenbank entspricht dann einer endlichen Struktur, deren Universum aus allen potentiellen Einträgen in einzelnen Zellen der Tabellen besteht, und die für jede Tabelle in der Datenbank eine Relation enthält.

Folie 168

## Beispiel: Eine Kinodatenbank

<i>Kino</i>			
Name	Adresse	Stadtteil	Telefonnummer
Babylon	Dresdner Str. 126	Kreuzberg	030 61 60 96 93
Casablanca	Friedenstr. 12-13	Adlershof	030 67 75 75 2
Filmtheater am Friedrichshain	Bötzowstr. 1-5	Prenzlauer Berg	030 42 84 51 88
Kino International	Karl-Marx-Allee 33	Mitte	030 24 75 60 11
Movimento	Kotbusser Damm 22	Kreuzberg	030 692 47 85
Urania	An der Urania 17	Schöneberg	030 21 89 09 1

<i>Film</i>		
Name	Regisseur	Schauspieler
Alien	Ridley Scott	Sigourney Weaver
Blade Runner	Ridley Scott	Harrison Ford
Blade Runner	Ridley Scott	Sean Young
Brazil	Terry Gilliam	Jonathan Pryce
Brazil	Terry Gilliam	Kim Greist
Casablanca	Michael Curtiz	Humphrey Bogart
Casablanca	Michael Curtiz	Ingrid Bergmann
Gravity	Alfonso Cuaron	Sandra Bullock
Gravity	Alfonso Cuaron	George Clooney
Monuments Men	George Clooney	George Clooney
Monuments Men	George Clooney	Matt Damon
Resident Evil	Paul Anderson	Milla Jovovich
Terminator	James Cameron	Arnold Schwarzenegger
Terminator	James Cameron	Linda Hamilton
Terminator	James Cameron	Michael Biehn
...	...	...

Folie 169

<i>Programm</i>		
Kino	Film	Zeit
Babylon	Casablanca	17:30
Babylon	Gravity	20:15
Casablanca	Blade Runner	15:30
Casablanca	Alien	18:15
Casablanca	Blade Runner	20:30
Casablanca	Resident Evil	20:30
Filmtheater am Friedrichshain	Resident Evil	20:00
Filmtheater am Friedrichshain	Resident Evil	21:30
Filmtheater am Friedrichshain	Resident Evil	23:00
Kino International	Casablanca	18:00
Kino International	Brazil	20:00
Kino International	Brazil	22:00
Movimento	Gravity	17:00
Movimento	Gravity	19:30
Movimento	Alien	22:00
Urania	Monuments Men	17:00
Urania	Monuments Men	20:00

Folie 170

## Die Kinodatenbank als Struktur

*Signatur:*  $\sigma_{\text{KINO}} := \{ R_{\text{Kino}}/4, R_{\text{Film}}/3, R_{\text{Prog}}/3 \} \cup \{ 'c' : c \in \text{ASCII}^* \}$



Die Kinodatenbank wird dargestellt als  $\sigma_{\text{KINO}}$ -Struktur  $\mathcal{D}$ .

*Universum:*

$D := \text{ASCII}^* \supseteq \{ \text{Babylon, Dresdner Str. 126, Kreuzberg, 030 61 60 96 93,} \\ \text{Casablanca, \dots, 20:00} \}.$

*Relationen:*

$R_{\text{Kino}}^{\mathcal{D}} := \{ (\text{Babylon, Dresdner Str. 126, Kreuzberg, 030 61 60 96 93}), \\ (\text{Casablanca, Friedenstr. 12-13, Adlershof, 030 67 75 75 2}), \\ (\text{Filmtheater am Friedrichshain, Böttzowstr. 1-5, Prenzlauer Berg, 030 42 84 51 88}), \\ (\text{Kino International, Karl-Marx-Allee 33, Mitte, 030 24 75 60 11}), \\ (\text{Movimiento, Kotbusser Damm 22, Kreuzberg, 030 692 47 85}), \\ (\text{Urania, An der Urania 17, Schöneberg, 030 21 89 09 1}) \}$

$R_{\text{Film}}^{\mathcal{D}} := \{ (\text{Alien, Ridley Scott, Sigourney Weaver}), \\ (\text{Blade Runner, Ridley Scott, Harrison Ford}), \dots \}$

$R_{\text{Prog}}^{\mathcal{D}} := \{ (\text{Babylon, Casablanca, 17:30}), \\ (\text{Babylon, Gravity, 20:15}), \dots \}.$

*Konstanten:* ‘ $c^{\mathcal{D}}$ ’ :=  $c$ , für jedes  $c \in \text{ASCII}^*$ .

D.h.: jedes Konstantensymbol wird durch den zwischen den Hochkommas stehenden Text interpretiert.

Folie 171

## Redukte und Expansionen

**Definition 3.5.** Seien  $\sigma$  und  $\tau$  Signaturen mit  $\sigma \subseteq \tau$ .

(a) Das  $\sigma$ -Redukt einer  $\tau$ -Struktur  $\mathcal{B}$  ist die  $\sigma$ -Struktur  $\mathcal{B}|_{\sigma}$  mit  $B|_{\sigma} := B$  und  $S^{\mathcal{B}|_{\sigma}} := S^{\mathcal{B}}$  für jedes  $S \in \sigma$ .

D.h.: Ist  $\mathcal{B} = (B, (S^{\mathcal{B}})_{S \in \tau})$ , so ist  $\mathcal{B}|_{\sigma} = (B, (S^{\mathcal{B}})_{S \in \sigma})$ .

(b) Eine  $\tau$ -Struktur  $\mathcal{B}$  ist eine  $\tau$ -Expansion einer  $\sigma$ -Struktur  $\mathcal{A}$ , wenn  $\mathcal{A} = \mathcal{B}|_{\sigma}$ .

**Beispiel.** Das  $\{+, \underline{0}\}$ -Redukt des Standardmodells der Arithmetik ist die Struktur

$$\mathcal{A}_{\mathbb{N}}|_{\{+, \underline{0}\}} = (\mathbb{N}, +^{\mathcal{A}_{\mathbb{N}}}, \underline{0}^{\mathcal{A}_{\mathbb{N}}}),$$

wobei  $+^{\mathcal{A}_{\mathbb{N}}}$  die natürliche Addition auf  $\mathbb{N}$  und  $\underline{0}^{\mathcal{A}_{\mathbb{N}}}$  die natürliche Zahl 0 ist. Man bezeichnet diese Struktur als das *Standardmodell der Presburger Arithmetik*.

Folie 172

## Prinzipielle Gleichheit von Strukturen

*Frage:* Wann sind zwei  $\sigma$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  „prinzipiell gleich“?

*Antwort:* Wenn  $\mathcal{B}$  aus  $\mathcal{A}$  entsteht, indem man die Elemente des Universums von  $\mathcal{A}$  umbenennt.

Dies wird in der folgenden Definition präzisiert.

Folie 173

## Isomorphismen

**Definition 3.6.** Seien  $\mathcal{A}$  und  $\mathcal{B}$   $\sigma$ -Strukturen. Ein *Isomorphismus* von  $\mathcal{A}$  nach  $\mathcal{B}$  ist eine Abbildung  $\pi : A \rightarrow B$  mit folgenden Eigenschaften:

1.  $\pi$  ist *bijektiv*.
2. Für alle  $k \in \mathbb{N} \setminus \{0\}$ , alle  $k$ -stelligen Relationssymbole  $R \in \sigma$  und alle  $k$ -Tupel  $(a_1, \dots, a_k) \in A^k$  gilt:

$$(a_1, \dots, a_k) \in R^{\mathcal{A}} \iff (\pi(a_1), \dots, \pi(a_k)) \in R^{\mathcal{B}}.$$

3. Für alle Konstantensymbole  $c \in \sigma$  gilt:

$$\pi(c^{\mathcal{A}}) = c^{\mathcal{B}}.$$

4. Für alle  $k \in \mathbb{N} \setminus \{0\}$ , alle  $k$ -stelligen Funktionssymbole  $f \in \sigma$  und alle  $k$ -Tupel  $(a_1, \dots, a_k) \in A^k$  gilt:

$$\pi(f^{\mathcal{A}}(a_1, \dots, a_k)) = f^{\mathcal{B}}(\pi(a_1), \dots, \pi(a_k)).$$

Folie 174

## Isomorphie

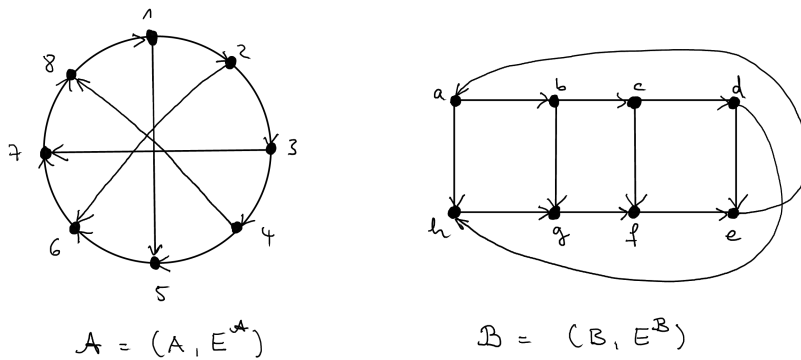
**Notation.** Seien  $\mathcal{A}$  und  $\mathcal{B}$   $\sigma$ -Strukturen. Wir schreiben  $\pi : \mathcal{A} \cong \mathcal{B}$ , um anzudeuten, dass  $\pi$  ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$  ist.

**Definition 3.7.** Zwei  $\sigma$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  heißen *isomorph* (wir schreiben:  $\mathcal{A} \cong \mathcal{B}$ ), wenn es einen Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$  gibt.

**Beispiele 3.8.**

(a) Seien  $A, B$  nicht-leere Mengen. Dann sind die  $\emptyset$ -Strukturen  $\mathcal{A} := (A)$  und  $\mathcal{B} := (B)$  genau dann isomorph, wenn  $A$  und  $B$  gleichmächtig sind (d.h. es gibt eine Bijektion von  $A$  nach  $B$ ).

(b) Seien  $\mathcal{A} = (A, E^{\mathcal{A}})$  und  $\mathcal{B} = (B, E^{\mathcal{B}})$  die beiden folgenden Digraphen:



Dann ist  $\pi : A \rightarrow B$  mit

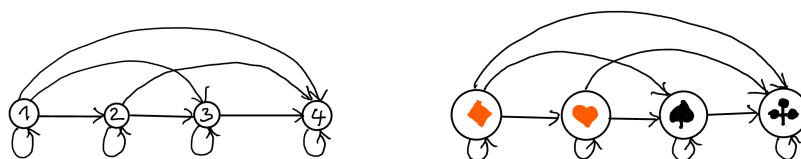
$i$	1	2	3	4	5	6	7	8
$\pi(i)$	$a$	$b$	$c$	$d$	$h$	$g$	$f$	$e$

ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$ .

(c) Sei  $\mathcal{A} = (A, \leq^{\mathcal{A}})$  mit  $A = \{1, 2, 3, 4\}$  und

$$\leq^{\mathcal{A}} = \{(i, j) : i, j \in \mathbb{N}, 1 \leq i \leq j \leq 4\},$$

und sei  $\mathcal{B} = (B, \leq^{\mathcal{B}})$  mit  $B = \{\diamond, \heartsuit, \spadesuit, \clubsuit\}$ , wobei  $\leq^{\mathcal{B}}$  wie in Beispiel 3.4 definiert ist. Skizze:



Dann ist  $\pi : A \rightarrow B$  mit

$i$	1	2	3	4
$\pi(i)$	◇	♥	♠	♣

ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$ .

*Allgemein gilt:* Sind  $A$  und  $B$  endliche Mengen mit  $|A| = |B|$ , und sind  $\leq^A$  und  $\leq^B$  lineare Ordnungen auf  $A$  und  $B$ , so ist die Abbildung  $\pi : A \rightarrow B$ , die das (bzgl.  $\leq^A$ ) kleinste Element in  $A$  auf das (bzgl.  $\leq^B$ ) kleinste Element in  $B$  abbildet, und allgemein für jedes  $i \in \{1, \dots, |A|\}$  das (bzgl.  $\leq^A$ )  $i$ -kleinste Element in  $A$  auf das (bzgl.  $\leq^B$ )  $i$ -kleinste Element in  $B$  abbildet, ein Isomorphismus von  $\mathcal{A} := (A, \leq^A)$  nach  $\mathcal{B} := (B, \leq^B)$ .

Folie 178

- (d) Sind  $\leq^{\mathbb{N}}$  und  $\leq^{\mathbb{Z}}$  die natürlichen linearen Ordnungen auf  $\mathbb{N}$  und  $\mathbb{Z}$ , so sind die  $\{\leq\}$ -Strukturen  $\mathcal{N} := (\mathbb{N}, \leq^{\mathbb{N}})$  und  $\mathcal{Z} := (\mathbb{Z}, \leq^{\mathbb{Z}})$  nicht isomorph (kurz:  $\mathcal{N} \not\cong \mathcal{Z}$ ).

*Beweis:* Angenommen,  $\pi : \mathbb{N} \rightarrow \mathbb{Z}$  ist ein Isomorphismus von  $\mathcal{N}$  nach  $\mathcal{Z}$ . Sei  $z := \pi(0)$ . In  $\mathbb{Z}$  gibt es ein Element  $z' \in \mathbb{Z}$  mit  $z' < z$  (z.B.  $z' = z - 1$ ). Da  $\pi$  surjektiv ist, muss es ein  $n' \in \mathbb{N}$  geben, so dass  $\pi(n') = z'$ . Wegen  $z' \neq z$  muss  $n' \neq 0$  gelten (da  $\pi$  injektiv ist). Somit gilt:

$$0 \leq^{\mathbb{N}} n' \quad \text{aber} \quad z \not\leq^{\mathbb{Z}} z'.$$

Also ist  $\pi$  kein Isomorphismus von  $\mathcal{N}$  nach  $\mathcal{Z}$ . Widerspruch!

Folie 179

- (e) Sei  $\sigma := \{f, c\}$ , wobei  $f$  ein 2-stelliges Funktionssymbol und  $c$  ein Konstantensymbol ist. Sei  $\mathcal{A} := (A, f^A, c^A)$ , wobei gilt:

- $A := \mathbb{N}$  ist die Menge aller natürlichen Zahlen,
- $f^A := +^{\mathbb{N}}$  ist die natürliche Addition auf  $\mathbb{N}$ ,
- $c^A := 0$  ist die natürliche Zahl 0

und sei  $\mathcal{B} := (B, f^B, c^B)$ , wobei

- $B := \{2^n : n \in \mathbb{N}\}$  ist die Menge aller Zweierpotenzen,

- $f^{\mathcal{B}} : B \times B \rightarrow B$  ist die Funktion mit

$$f^{\mathcal{B}}(b_1, b_2) := b_1 \cdot b_2, \quad \text{für alle } b_1, b_2 \in B$$

- $c^{\mathcal{B}} := 1 = 2^0 \in B$ .

Dann gilt:  $\mathcal{A} \cong \mathcal{B}$ , und die Abbildung  $\pi : A \rightarrow B$  mit  $\pi(n) := 2^n$  für alle  $n \in \mathbb{N}$  ist ein *Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$* , denn:

1.  $\pi$  ist eine bijektive Abbildung von  $A$  nach  $B$ .
2. Für das Konstantensymbol  $c \in \sigma$  gilt:

$$\pi(c^{\mathcal{A}}) = \pi(0) = 2^0 = c^{\mathcal{B}}.$$

3. Für das Funktionssymbol  $f \in \sigma$  und für alle  $(a_1, a_2) \in A^2$  gilt:

$$\pi(f^{\mathcal{A}}(a_1, a_2)) = \pi(a_1 + a_2) = 2^{a_1+a_2}$$

und

$$f^{\mathcal{B}}(\pi(a_1), \pi(a_2)) = f^{\mathcal{B}}(2^{a_1}, 2^{a_2}) = 2^{a_1} \cdot 2^{a_2} = 2^{a_1+a_2},$$

$$\text{also } \pi(f^{\mathcal{A}}(a_1, a_2)) = f^{\mathcal{B}}(\pi(a_1), \pi(a_2)).$$

Somit ist  $\pi$  ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$ .

Folie 180

## Isomorphie ist eine Äquivalenzrelation

**Lemma 3.9.** *Isomorphie ist eine Äquivalenzrelation auf der Klasse aller  $\sigma$ -Strukturen. D.h.: Für alle  $\sigma$ -Strukturen  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  gilt:*

1.  $\mathcal{A} \cong \mathcal{A}$  (Reflexivität),
2.  $\mathcal{A} \cong \mathcal{B} \implies \mathcal{B} \cong \mathcal{A}$  (Symmetrie),
3.  $\mathcal{A} \cong \mathcal{B}$  und  $\mathcal{B} \cong \mathcal{C} \implies \mathcal{A} \cong \mathcal{C}$  (Transitivität).

*Beweis:* Übung.

## 3.2 Terme der Logik erster Stufe

Folie 181

### Individuenvariablen

**Definition 3.10.** Eine *Individuenvariable* (auch: *Variable erster Stufe*; kurz: *Variable*) hat die Form  $v_i$  für ein  $i \in \mathbb{N}$ .

Die Menge aller Variablen bezeichnen wir mit VAR, d.h.

$$\text{VAR} = \{v_0, v_1, v_2, v_3, \dots\} = \{v_i : i \in \mathbb{N}\}.$$

Folie 182

### Terme der Logik erster Stufe

#### Definition 3.11.

- (a) Für eine Signatur  $\sigma$  sei  $A_{\sigma\text{-Terme}}$  das *Alphabet*, das aus allen Elementen in VAR, allen *Konstanten- und Funktionssymbolen in  $\sigma$* , den Klammern  $(, )$  und dem Komma  $,$  besteht.
- (b) Die Menge  $T_\sigma$  aller  $\sigma$ -*Terme* ist die wie folgt rekursiv definierte Teilmenge von  $A_{\sigma\text{-Terme}}^*$ :

*Basisregeln:*

- Für jedes Konstantensymbol  $c \in \sigma$  ist  $c \in T_\sigma$ .
- Für jede Variable  $x \in \text{VAR}$  ist  $x \in T_\sigma$ .

*Rekursive Regel:*

- Für jedes Funktionssymbol  $f \in \sigma$  und für  $k := \text{ar}(f)$  gilt:  
Sind  $t_1 \in T_\sigma, \dots, t_k \in T_\sigma$ , so ist auch  $f(t_1, \dots, t_k) \in T_\sigma$ .

- (c) Die Menge aller *Terme der Logik der ersten Stufe* ist  $T := \bigcup_{\sigma \text{ Signatur}} T_\sigma$ .

Folie 183

## Beispiele

Sei  $\sigma := \{ f/2, c \}$ .

Folgende Worte sind  $\sigma$ -Terme:

$$c, \quad v_4, \quad f(c, c), \quad f(c, f(c, v_0)).$$

Folgende Worte sind keine  $\sigma$ -Terme:

$$0, \quad f(0, c), \quad f(v_0, c, v_1), \quad f^A(2, 3).$$

Folie 184

## Belegungen und Interpretationen

**Definition 3.12.** Sei  $\sigma$  eine Signatur.

(a) Eine *Belegung in einer  $\sigma$ -Struktur  $\mathcal{A}$*  ist eine Abbildung  $\beta : \text{VAR} \rightarrow A$ .

D.h.:  $\beta$  ordnet jeder Variablen  $x \in \text{VAR}$  ein Element  $\beta(x)$  aus dem Universum von  $\mathcal{A}$  zu.

(b) Eine  *$\sigma$ -Interpretation* ist ein Paar

$$\mathcal{I} = (\mathcal{A}, \beta),$$

bestehend aus einer  $\sigma$ -Struktur  $\mathcal{A}$  und einer Belegung  $\beta$  in  $\mathcal{A}$ .

Folie 185

## Die Auswertung von Termen in Interpretationen

Wir wollen Terme nun in Interpretationen „auswerten“.

Die Auswertung von Term  $t$  in einer Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  soll dasjenige Element aus  $A$  liefern, das man erhält, wenn man

- die in  $t$  vorkommenden **Variablen** gemäß der Belegung  $\beta$  interpretiert,
- die in  $t$  vorkommenden Konstantensymbole  $c$  gemäß ihrer Interpretation  $c^{\mathcal{A}}$  in  $\mathcal{A}$  belegt,
- die in  $t$  vorkommenden Funktionssymbole  $f$  gemäß ihrer Interpretation  $f^{\mathcal{A}}$  in  $\mathcal{A}$  belegt

und dann nach und nach den resultierenden Term ausrechnet.

Dies wird in der folgenden Definition präzisiert.

Folie 186

## Semantik von $\sigma$ -Termen

**Definition 3.13.** Sei  $\sigma$  eine Signatur.

Rekursiv über den Aufbau von  $\mathbb{T}_\sigma$  definieren wir eine Funktion  $\llbracket \cdot \rrbracket$ , die jedem  $\sigma$ -Term  $t$  und jeder  $\sigma$ -Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  einen Wert  $\llbracket t \rrbracket^{\mathcal{I}} \in A$  zuordnet:

- Für alle  $x \in \text{VAR}$  ist  $\llbracket x \rrbracket^{\mathcal{I}} := \beta(x)$ .
- Für alle Konstantensymbole  $c \in \sigma$  ist  $\llbracket c \rrbracket^{\mathcal{I}} := c^{\mathcal{A}}$ .
- Für alle Funktionssymbole  $f \in \sigma$ , für  $k := \text{ar}(f)$ , und für alle  $\sigma$ -Terme  $t_1, \dots, t_k \in \mathbb{T}_\sigma$  gilt:

$$\llbracket f(t_1, \dots, t_k) \rrbracket^{\mathcal{I}} := f^{\mathcal{A}}(\llbracket t_1 \rrbracket^{\mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\mathcal{I}}).$$

Folie 187

## Beispiel

Sei  $\sigma = \{ f/2, c \}$ , und sei  $\mathcal{A} = (A, f^{\mathcal{A}}, c^{\mathcal{A}})$  die  $\sigma$ -Struktur mit  $A = \mathbb{N}$ ,  $f^{\mathcal{A}} = +^{\mathbb{N}}$  (die Addition auf den natürlichen Zahlen) und  $c^{\mathcal{A}} = 0$  (die natürliche Zahl 0).

Sei  $\beta : \text{VAR} \rightarrow A$  eine Belegung mit  $\beta(v_1) = 1$  und  $\beta(v_2) = 7$ , und sei  $\mathcal{I} := (\mathcal{A}, \beta)$ .

Sei  $t$  der  $\sigma$ -Term  $f(v_2, f(v_1, c))$ . Dann gilt:

$$\begin{aligned} \llbracket t \rrbracket^{\mathcal{I}} &= f^{\mathcal{A}}(\beta(v_2), f^{\mathcal{A}}(\beta(v_1), c^{\mathcal{A}})) \\ &= f^{\mathcal{A}}(7, f^{\mathcal{A}}(1, 0)) \\ &= (7 + (1 + 0)) \\ &= 8. \end{aligned}$$

## 3.3 Syntax der Logik erster Stufe

Folie 188

### Vergleich zwischen Aussagenlogik und Logik erster Stufe

Die Logik erster Stufe übernimmt, verändert und erweitert die Syntax der Aussagenlogik.



- Was gleich bleibt:
  - Die Junktoren  $\neg, \wedge, \vee, \rightarrow$  werden übernommen.
- Was sich verändert:
  - *Variablen stehen nicht mehr für „wahre“ oder „falsche“ Aussagen, sondern für Elemente im Universum einer  $\sigma$ -Struktur.*
  - *Variablen sind keine atomaren Formeln mehr.*
- Was neu hinzukommt:
  - Es gibt *Quantoren*  $\exists$  und  $\forall$  (für „es existiert“ und „für alle“).
  - Es gibt Symbole für Elemente aus der Signatur  $\sigma$ .
  - Es können  $\sigma$ -Terme benutzt werden, um Elemente im Universum einer  $\sigma$ -Struktur zu bezeichnen.

Folie 189

## Das Alphabet der Logik erster Stufe

**Definition 3.14.** Sei  $\sigma$  eine Signatur.

Das *Alphabet*  $A_{\text{FO}[\sigma]}$  der Logik erster Stufe über  $\sigma$  besteht aus

- allen Symbolen in  $A_{\sigma\text{-Terme}}$ ,
- allen Symbolen in  $\sigma$ ,
- den Quantoren  $\exists$  (Existenzquantor) und  $\forall$  (Allquantor),
- dem Gleichheitssymbol  $=$ ,
- den Junktoren  $\neg, \wedge, \vee, \rightarrow$ .

D.h.:

$$A_{\text{FO}[\sigma]} = \text{VAR} \cup \sigma \cup \{\exists, \forall\} \cup \{=\} \cup \{\neg, \wedge, \vee, \rightarrow\} \cup \{(, )\} \cup \{, \}.$$

Folie 190

## Syntax der Logik erster Stufe

**Definition 3.15.** Sei  $\sigma$  eine Signatur.

Die Menge  $\text{FO}[\sigma]$  aller *Formeln der Logik erster Stufe über der Signatur  $\sigma$*  (kurz:  $\text{FO}[\sigma]$ -Formeln; „FO“ steht für die englische Bezeichnung der Logik erster Stufe: first-order logic) ist die folgendermaßen rekursiv definierte Teilmenge von  $A_{\text{FO}[\sigma]}^*$ :

*Basisregeln:*

- Für alle  $\sigma$ -Terme  $t_1$  und  $t_2$  in  $\mathbb{T}_\sigma$  gilt:

$$t_1 = t_2 \in \text{FO}[\sigma].$$

- Für jedes Relationssymbol  $R \in \sigma$ , für  $k := \text{ar}(R)$  und für alle  $\sigma$ -Terme  $t_1, \dots, t_k$  in  $\mathbb{T}_\sigma$  gilt:

$$R(t_1, \dots, t_k) \in \text{FO}[\sigma].$$

$\text{FO}[\sigma]$ -Formeln der Form  $t_1 = t_2$  oder  $R(t_1, \dots, t_k)$  heißen *atomare  $\sigma$ -Formeln*.

Folie 191

*Rekursive Regeln:*

- Ist  $\varphi \in \text{FO}[\sigma]$ , so ist auch  $\neg\varphi \in \text{FO}[\sigma]$ .
- Ist  $\varphi \in \text{FO}[\sigma]$  und  $\psi \in \text{FO}[\sigma]$ , so ist auch
  - $(\varphi \wedge \psi) \in \text{FO}[\sigma]$ ,
  - $(\varphi \vee \psi) \in \text{FO}[\sigma]$ ,
  - $(\varphi \rightarrow \psi) \in \text{FO}[\sigma]$ .
- Ist  $\varphi \in \text{FO}[\sigma]$  und  $x \in \text{VAR}$ , so ist auch
  - $\exists x \varphi \in \text{FO}[\sigma]$ ,
  - $\forall x \varphi \in \text{FO}[\sigma]$ .

Folie 192

**Beispiel 3.16.** Sei  $\sigma = \{ f/2, c \}$ .

Folgende Worte aus  $A_{\text{FO}[\sigma]}^*$  sind  $\text{FO}[\sigma]$ -Formeln:

- $f(v_0, v_1) = c$  (atomare  $\sigma$ -Formel)
- $\forall v_2 f(v_2, c) = v_2$
- $\neg \exists v_3 (f(v_3, v_3) = v_3 \wedge \neg v_3 = c)$

Folgende Worte sind keine FO[ $\sigma$ ]-Formeln:

- $(f(v_0, v_1) = c)$
- $(\exists v_2 f(v_2, c) = v_2)$
- $f(f(c, c), v_1)$  (ist ein  $\sigma$ -Term, aber keine FO[ $\sigma$ ]-Formel)
- $\exists c f(v_0, c) = v_0$

Folie 193

**Beispiel 3.17.** Sei  $\sigma = \{E/2\}$ .

Folgendes ist eine FO[ $\sigma$ ]-Formel:

$$\forall v_0 \forall v_1 \left( (E(v_0, v_1) \wedge E(v_1, v_0)) \rightarrow v_0 = v_1 \right)$$

*Intuition zur Semantik:*

In einem gerichteten Graphen  $\mathcal{A} = (A, E^{\mathcal{A}})$  sagt diese Formel Folgendes aus:

„Für alle Knoten  $a_0 \in A$  und  
für alle Knoten  $a_1 \in A$  gilt:  
falls  $(a_0, a_1) \in E^{\mathcal{A}}$  und  $(a_1, a_0) \in E^{\mathcal{A}}$ , so ist  $a_0 = a_1$ .“

Die Formel sagt in einem Digraph  $\mathcal{A} = (A, E^{\mathcal{A}})$  also aus, dass die Kantenrelation  $E^{\mathcal{A}}$  antisymmetrisch ist.

Folie 194

## Notation

- Statt mit  $v_0, v_1, v_2, \dots$  bezeichnen wir Variablen oft auch mit  $x, y, z, \dots$  oder mit Varianten wie  $x', y_1, y_2, \dots$
- Ähnlich wie bei der Aussagenlogik schreiben wir  $(\varphi \leftrightarrow \psi)$  als Abkürzung für die Formel  $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$ .
- Die Menge aller *Formeln der Logik der ersten Stufe* ist

$$\text{FO} := \bigcup_{\sigma \text{ Signatur}} \text{FO}[\sigma].$$

### 3.4 Semantik der Logik erster Stufe

Folie 195

Bevor wir die Semantik der Logik erster Stufe formal definieren, betrachten wir zunächst einige Beispiele, um ein intuitives Verständnis der Semantik der Logik erster Stufe zu erlangen.

#### *Beispiele zur Semantik der Logik erster Stufe*

Folie 196

#### Gerichtete Graphen

**Beispiel 3.18.** Sei  $\sigma = \{E/2\}$ .

(a) Die FO[ $\sigma$ ]-Formel

$$\varphi := \forall x \forall y (E(x, y) \rightarrow E(y, x))$$

besagt:

„Für alle Knoten  $x$  und für alle Knoten  $y$  gilt: Falls es eine Kante von  $x$  nach  $y$  gibt, so gibt es auch eine Kante von  $y$  nach  $x$ .“

Für jeden Digraphen  $\mathcal{A} = (A, E^{\mathcal{A}})$  gilt daher:

$$\mathcal{A} \text{ erfüllt } \varphi \iff E^{\mathcal{A}} \text{ ist symmetrisch.}$$

Umgangssprachlich sagen wir auch: „Die Formel  $\varphi$  sagt in einem Digraphen  $\mathcal{A}$  aus, dass dessen Kantenrelation symmetrisch ist.“

Folie 197

(b) Die folgende FO[ $\sigma$ ]-Formel drückt aus, dass es von Knoten  $x$  zu Knoten  $y$  einen Weg der Länge 3 gibt:

$$\varphi(x, y) := \exists z_1 \exists z_2 \left( (E(x, z_1) \wedge E(z_1, z_2)) \wedge E(z_2, y) \right).$$

(c) Die FO[ $\sigma$ ]-Formel

$$\forall x \forall y \exists z_1 \exists z_2 \left( (E(x, z_1) \wedge E(z_1, z_2)) \wedge E(z_2, y) \right)$$

sagt in einem Digraph  $\mathcal{A}$  aus, dass es zwischen je 2 Knoten einen Weg der Länge 3 gibt.

Folie 198

## Verwandtschaftsbeziehungen

Wir betrachten eine Datensammlung, in der die Stammbäume von Pferden aus dem Sport *Dressurreiten* verwaltet werden.

Um Verwandtschaftsbeziehungen zwischen den Pferden zu modellieren, können wir eine Signatur  $\sigma$  nutzen, die aus den folgenden Symbolen besteht:

- 1-stellige Funktionssymbole *Vater*, *Mutter*  
(Bedeutung:  $x = \text{Mutter}(y)$  besagt: „ $x$  ist die Mutter von  $y$ “.)
- 2-stellige Relationssymbole *Geschwister*, *Vorfahr*  
(Bedeutung:  $\text{Geschwister}(x, y)$  besagt, dass  $x$  und  $y$  Geschwister sind;  
 $\text{Vorfahr}(x, y)$  besagt, dass  $x$  ein Vorfahr von  $y$  ist.)

Generelles Wissen über Verwandtschaftsbeziehungen lässt sich durch Formeln der Logik erster Stufe repräsentieren, z.B.:

- „Pferde mit gleichem Vater und gleicher Mutter sind Geschwister“:

$$\forall x \forall y \left( \left( \text{Vater}(x) = \text{Vater}(y) \wedge \text{Mutter}(x) = \text{Mutter}(y) \right) \wedge \neg x = y \right) \rightarrow \text{Geschwister}(x, y)$$

Folie 199

- „Eltern sind gerade die unmittelbaren Vorfahren“:

$$\forall x \forall y \left( \left( x = \text{Vater}(y) \vee x = \text{Mutter}(y) \right) \leftrightarrow \left( \text{Vorfahr}(x, y) \wedge \neg \exists z \left( \text{Vorfahr}(x, z) \wedge \text{Vorfahr}(z, y) \right) \right) \right)$$

- „Die Relation *Vorfahr* ist transitiv“:

$$\forall x \forall y \forall z \left( \left( \text{Vorfahr}(x, y) \wedge \text{Vorfahr}(y, z) \right) \rightarrow \text{Vorfahr}(x, z) \right)$$

- Die folgende Formel  $\varphi(x, y)$  besagt „ $x$  ist Tante oder Onkel von  $y$ “:

$$\varphi(x, y) := \exists z \left( \text{Geschwister}(x, z) \wedge \left( z = \text{Mutter}(y) \vee z = \text{Vater}(y) \right) \right)$$

Folie 200

- Die folgende Formel  $\psi(x)$  besagt „ $x$  ist Vater von genau 2 Kindern“:

$$\psi(x) := \exists y_1 \exists y_2 \left( ((x = \text{Vater}(y_1) \wedge x = \text{Vater}(y_2)) \wedge \neg y_1 = y_2) \wedge \forall z (x = \text{Vater}(z) \rightarrow (z = y_1 \vee z = y_2)) \right)$$

### Formale Definition der Semantik der Logik erster Stufe

Folie 201

Um die formale Definition der Semantik der Logik erster Stufe angeben zu können, benötigen wir noch folgende Begriffe:

Folie 202

#### Notation

- Ist  $\beta$  eine Belegung in einer  $\sigma$ -Struktur  $\mathcal{A}$ , ist  $x \in \text{VAR}$  und ist  $a \in A$ , so sei

$$\beta_x^a$$

die Belegung mit  $\beta_x^a(x) = a$  und  $\beta_x^a(y) = \beta(y)$  für alle  $y \in \text{VAR} \setminus \{x\}$ .

- Ist  $\mathcal{I} = (\mathcal{A}, \beta)$  eine  $\sigma$ -Interpretation, ist  $x \in \text{VAR}$  und ist  $a \in A$ , so sei

$$\mathcal{I}_x^a := (\mathcal{A}, \beta_x^a).$$

Folie 203

### Semantik der Logik erster Stufe

**Definition 3.19.** Sei  $\sigma$  eine Signatur.

Rekursiv über den Aufbau von  $\text{FO}[\sigma]$  definieren wir eine Funktion  $\llbracket \cdot \rrbracket$ , die jeder  $\text{FO}[\sigma]$ -Formel  $\varphi$  und jeder  $\sigma$ -Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  einen Wahrheitswert (kurz: Wert)  $\llbracket \varphi \rrbracket^{\mathcal{I}} \in \{0, 1\}$  zuordnet:

*Rekursionsanfang:*

- Für alle  $\sigma$ -Terme  $t_1$  und  $t_2$  in  $T_\sigma$  gilt:

$$\llbracket t_1 = t_2 \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls } \llbracket t_1 \rrbracket^{\mathcal{I}} = \llbracket t_2 \rrbracket^{\mathcal{I}} \\ 0, & \text{sonst.} \end{cases}$$

- Für jedes Relationssymbol  $R \in \sigma$ , für  $k := \text{ar}(R)$  und für alle  $\sigma$ -Terme  $t_1, \dots, t_k \in T_\sigma$  gilt:

$$\llbracket R(t_1, \dots, t_k) \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls } (\llbracket t_1 \rrbracket^{\mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\mathcal{I}}) \in R^{\mathcal{A}} \\ 0, & \text{sonst.} \end{cases}$$

*Rekursionsschritt:*

Folie 204

- Ist  $\varphi \in \text{FO}[\sigma]$  und ist  $x \in \text{VAR}$ , so ist

$$\llbracket \exists x \varphi \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls es (mind.) ein } a \in A \text{ gibt, so dass } \llbracket \varphi \rrbracket^{\mathcal{I}_x^a} = 1 \\ 0, & \text{sonst} \end{cases}$$

$$\llbracket \forall x \varphi \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls für jedes } a \in A \text{ gilt: } \llbracket \varphi \rrbracket^{\mathcal{I}_x^a} = 1 \\ 0, & \text{sonst} \end{cases}$$

Folie 205

- Die Semantik der Junktoren  $\neg, \wedge, \vee, \rightarrow$  ist wie in der Aussagenlogik definiert, d.h. für alle  $\varphi \in \text{FO}[\sigma]$  und  $\psi \in \text{FO}[\sigma]$  gilt:

$$\llbracket \neg \varphi \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 0 \\ 0, & \text{sonst} \end{cases}$$

$$\llbracket (\varphi \wedge \psi) \rrbracket^{\mathcal{I}} := \begin{cases} 1, & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 1 \text{ und } \llbracket \psi \rrbracket^{\mathcal{I}} = 1 \\ 0, & \text{sonst} \end{cases}$$

$$\llbracket (\varphi \vee \psi) \rrbracket^{\mathcal{I}} := \begin{cases} 0, & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 0 \text{ und } \llbracket \psi \rrbracket^{\mathcal{I}} = 0 \\ 1, & \text{sonst} \end{cases}$$

$$\llbracket (\varphi \rightarrow \psi) \rrbracket^{\mathcal{I}} := \begin{cases} 0, & \text{falls } \llbracket \varphi \rrbracket^{\mathcal{I}} = 1 \text{ und } \llbracket \psi \rrbracket^{\mathcal{I}} = 0 \\ 1, & \text{sonst} \end{cases}$$

Folie 206

**Beispiel 3.20.** Sei  $\sigma = \{E/2\}$ . Betrachte die FO[ $\sigma$ ]-Formel

$$\varphi := \forall x \forall y (E(x, y) \rightarrow E(y, x))$$

Für jede  $\sigma$ -Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  gilt:

$$\begin{aligned} \llbracket \varphi \rrbracket^{\mathcal{I}} = 1 &\iff \text{für alle } a \in A \text{ gilt: } \llbracket \forall y (E(x, y) \rightarrow E(y, x)) \rrbracket^{\mathcal{I}}_{\frac{a}{x}} = 1 \\ &\iff \text{für alle } a \in A \text{ gilt: für alle } b \in A \text{ gilt:} \\ &\quad \llbracket (E(x, y) \rightarrow E(y, x)) \rrbracket^{\mathcal{I}}_{\frac{a}{x} \frac{b}{y}} = 1 \\ &\iff \text{für alle } a \in A \text{ und alle } b \in A \text{ gilt:} \\ &\quad \text{Falls } \llbracket E(x, y) \rrbracket^{\mathcal{I}}_{\frac{a}{x} \frac{b}{y}} = 1, \text{ so } \llbracket E(y, x) \rrbracket^{\mathcal{I}}_{\frac{a}{x} \frac{b}{y}} = 1 \\ &\iff \text{für alle } a \in A \text{ und alle } b \in B \text{ gilt:} \\ &\quad \text{Falls } (a, b) \in E^{\mathcal{A}}, \text{ so } (b, a) \in E^{\mathcal{A}} \\ &\iff E^{\mathcal{A}} \text{ ist symmetrisch} \end{aligned}$$

Folie 207

## Die Modellbeziehung

**Definition 3.21.** Sei  $\sigma$  eine Signatur.

- Eine  $\sigma$ -Interpretation  $\mathcal{I}$  *erfüllt* eine Formel  $\varphi \in \text{FO}[\sigma]$  (wir schreiben:  $\mathcal{I} \models \varphi$ ), wenn  $\llbracket \varphi \rrbracket^{\mathcal{I}} = 1$ .
- Eine  $\sigma$ -Interpretation  $\mathcal{I}$  *erfüllt* eine Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  (wir schreiben:  $\mathcal{I} \models \Phi$ ), wenn  $\mathcal{I} \models \varphi$  für alle  $\varphi \in \Phi$  gilt.
- Ein *Modell* einer Formel  $\varphi$  (bzw. einer Formelmenge  $\Phi$ ) ist eine Interpretation  $\mathcal{I}$  mit  $\mathcal{I} \models \varphi$  (bzw.  $\mathcal{I} \models \Phi$ ).

Folie 208

## Konventionen

- Terme bezeichnen wir mit  $t, s$  und Varianten  $s', t_1, t_2, \dots$
- Formeln bezeichnen wir mit  $\varphi, \psi, \chi$  und Varianten  $\psi', \varphi_1, \varphi_2, \dots$
- Formelmengen bezeichnen wir mit  $\Phi, \Psi$  und Varianten  $\Psi', \Phi_1, \Phi_2, \dots$

Folie 209



## Subformeln, Subterme und Syntaxbäume

- Eine Formel  $\psi$  ist *Subformel* einer Formel  $\varphi$ , wenn  $\psi$  als Teilwort in  $\varphi$  vorkommt (insbes. ist jede Formel eine Subformel von sich selbst).

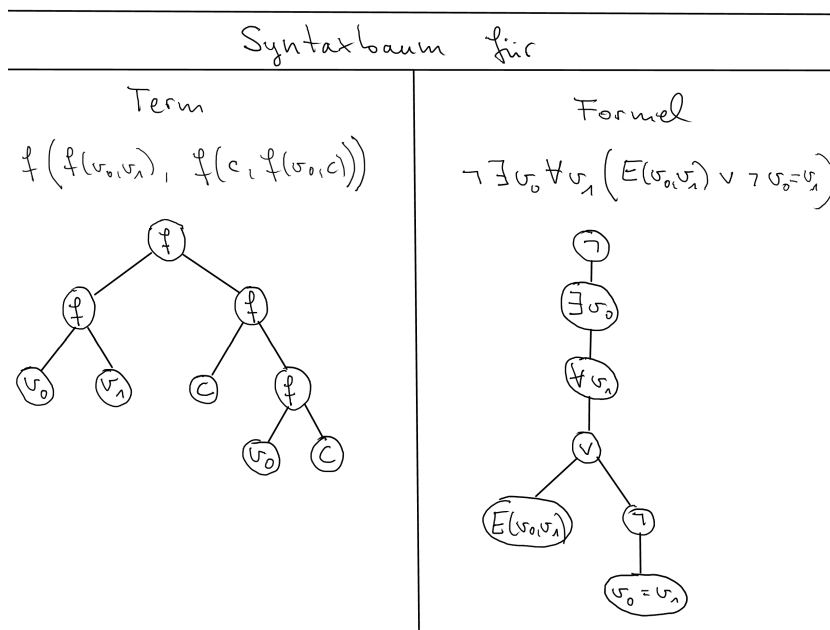
*Beispiel:*  $\psi := E(v_0, v_1)$  ist Subformel der Formel  $\exists v_0 \forall v_1 E(v_0, v_1)$

- Ein Term  $s$  ist *Subterm* eines Terms  $t$ , wenn  $s$  als Teilwort in  $t$  vorkommt (insbes. ist jeder Term ein Subterm von sich selbst).

*Beispiel:*  $f(c, c)$  ist Subterm des Terms  $f(v_0, f(c, c))$ .

- Sei  $\xi \in \mathsf{T} \cup \mathsf{FO}$ , d.h.  $\xi$  ist ein Term oder eine Formel der Logik erster Stufe.
  - Ähnlich wie bei aussagenlogischen Formeln können wir einen *Syntaxbaum* für  $\xi$  definieren.
  - Das *Lemma über die eindeutige Lesbarkeit von Termen und Formeln* besagt, dass jeder Term und jede Formel genau einen Syntaxbaum hat.
  - Die *Subterme* von  $\xi$  (falls  $\xi \in \mathsf{T}$ ) bzw. *Subformeln* von  $\xi$  (falls  $\xi \in \mathsf{FO}$ ) sind dann alle Terme bzw. Formeln, die im Syntaxbaum vorkommen.

*Beispiel:*



## Das Isomorphielemma

Folie 210

Das *Isomorphielemma* besagt, dass isomorphe Objekte (Strukturen bzw. Interpretationen) dieselben Formeln der Logik erster Stufe erfüllen.

Um diese Aussage präzise formulieren zu können, benötigen wir die folgende Notation.

Folie 211

### Isomorphismen, Belegungen und Interpretationen

**Definition 3.22.** Sei  $\sigma$  eine Signatur, seien  $\mathcal{A}, \mathcal{B}$  isomorphe  $\sigma$ -Strukturen und sei  $\pi$  ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$  (kurz:  $\pi : \mathcal{A} \cong \mathcal{B}$ ).

(a) Für jede Belegung  $\beta$  in  $\mathcal{A}$  sei  $\pi\beta$  die Belegung in  $\mathcal{B}$ , so dass für alle  $x \in \text{VAR}$  gilt:

$$\pi\beta(x) = \pi(\beta(x)).$$

(b) Für eine Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  schreiben wir  $\pi\mathcal{I}$  für die Interpretation

$$\pi\mathcal{I} := (\mathcal{B}, \pi\beta).$$

Aus dieser Definition folgt direkt:

**Lemma 3.23.** Sei  $\sigma$  eine Signatur, seien  $\mathcal{A}, \mathcal{B}$  isomorphe  $\sigma$ -Strukturen, sei  $\pi : \mathcal{A} \cong \mathcal{B}$ , sei  $\beta$  eine Belegung in  $\mathcal{A}$  und sei  $\mathcal{I} := (\mathcal{A}, \beta)$ . Für jedes  $x \in \text{VAR}$ , für jedes  $a \in A$ , für  $\mathcal{I}' := \mathcal{I}_x^a$  und für  $b := \pi(a)$  gilt:

$$\pi\mathcal{I}' = (\pi\mathcal{I})_x^b.$$

*Beweis.* Sei  $\beta' := \beta_x^a$ . Somit ist  $\mathcal{I}' = (\mathcal{A}, \beta')$  und daher  $\pi\mathcal{I}' = (\mathcal{B}, \pi\beta')$ . Andererseits ist  $(\pi\mathcal{I})_x^b = (\mathcal{B}, (\pi\beta)_x^b)$ . Wir müssen also zeigen, dass  $\pi\beta' = (\pi\beta)_x^b$ . D.h., wir müssen für jede Variable  $z \in \text{VAR}$  zeigen, dass gilt:

$$(\pi\beta')(z) = ((\pi\beta)_x^b)(z).$$

Wir betrachten zunächst die Variable  $z := x$ . Es gilt:

- $((\pi\beta)_x^b)(x) = b$ .
- $(\pi\beta')(x) = \pi(\beta'(x)) = \pi(\beta_x^a(x)) = \pi(a) = b$ .

Somit ist  $(\pi\beta')(x) = ((\pi\beta)\frac{b}{x})(x)$ .

Betrachte nun eine beliebige Variable  $z \neq x$ . Es gilt:

- $((\pi\beta)\frac{b}{x})(z) = (\pi\beta)(z) = \pi(\beta(z))$ .
- $(\pi\beta')(z) = \pi(\beta'(z)) = \pi(\beta\frac{a}{x}(z)) = \pi(\beta(z))$ .

Somit ist  $(\pi\beta')(z) = ((\pi\beta)\frac{b}{x})(z)$  für alle  $z \in \text{VAR} \setminus \{x\}$ . □

Folie 212

## Das Isomorphielemma

**Satz 3.24** (Das Isomorphielemma der Logik erster Stufe).

Sei  $\sigma$  eine Signatur, seien  $\mathcal{A}, \mathcal{B}$  isomorphe  $\sigma$ -Strukturen und sei  $\pi : \mathcal{A} \cong \mathcal{B}$ .

Für jede Belegung  $\beta$  in  $\mathcal{A}$  und die  $\sigma$ -Interpretation  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:

- (a) Für jeden  $\sigma$ -Term  $t \in \mathsf{T}_\sigma$  ist  $\llbracket t \rrbracket^{\pi\mathcal{I}} = \pi(\llbracket t \rrbracket^{\mathcal{I}})$ .
- (b) Für jede  $\text{FO}[\sigma]$ -Formel  $\varphi$  gilt:  $\pi\mathcal{I} \models \varphi \iff \mathcal{I} \models \varphi$ .

Wir werden das Isomorphielemma per Induktion über den Aufbau von Termen und Formeln beweisen. Hierzu zunächst ein kurzer Überblick darüber, wie solche Induktionsbeweise prinzipiell aufgebaut sind.

Folie 213

## Beweise per Induktion über den Aufbau von Termen und Formeln

- Ähnlich wie Aussagen über die aussagenlogischen Formeln können wir Aussagen über Terme und Formeln der Logik der ersten Stufe per *Induktion über den Aufbau* von  $\mathsf{T}_\sigma$  bzw.  $\text{FO}[\sigma]$  beweisen.
- Im *Induktionsanfang* beweisen wir die Aussagen für die gemäß Basisregeln definierten Terme bzw. Formeln. Im *Induktionsschritt* schließen wir von den Subtermen bzw. Subformeln auf den Term bzw. die Formel selbst.
- Wie bei der Aussagenlogik ist dieses Vorgehen gerechtfertigt, weil es sich auch als vollständige Induktion über die Höhe des Syntaxbaums auffassen lässt.

Folie 214

## Beweise per Induktion über den Aufbau von Termen

Schematisch sieht der Beweis einer Aussage  $\mathbb{A}(t)$  für alle Terme  $t \in \mathsf{T}_\sigma$  wie folgt aus:

*Induktionsanfang:*

- Beweise, dass für alle *Konstantensymbole*  $c \in \sigma$  die Aussage  $\mathbb{A}(c)$  gilt.
- Beweise, dass für alle *Variablen*  $x \in \mathsf{VAR}$  die Aussage  $\mathbb{A}(x)$  gilt.

*Induktionsschritt:*

- Betrachte jedes *Funktionssymbol*  $f \in \sigma$ , sei  $k := \text{ar}(f)$ , und seien  $t_1, \dots, t_k$  beliebige  $\sigma$ -Terme. Beweise, dass  $\mathbb{A}(f(t_1, \dots, t_k))$  gilt, und verwende dazu die *Induktionsannahme*, dass  $\mathbb{A}(t_i)$  für jedes  $i \in [k]$  gilt.

Mit dieser Vorgehensweise beweisen wir nun Teil (a) des Isomorphielemmas.

### *Beweis von Teil (a) von Satz 3.24 (Isomorphielemma).*

Per Induktion über den Aufbau von Termen. Die Aussage  $\mathbb{A}(t)$ , die wir für alle Terme  $t \in \mathsf{T}_\sigma$  beweisen wollen, besagt:  $\llbracket t \rrbracket^{\pi \mathcal{I}} = \pi(\llbracket t \rrbracket^{\mathcal{I}})$ .

*Induktionsanfang:*

- Sei  $c \in \sigma$  ein Konstantensymbol. **Behauptung:**  $\llbracket c \rrbracket^{\pi \mathcal{I}} = \pi(\llbracket c \rrbracket^{\mathcal{I}})$ .  
*Beweis:* Es gilt  $\llbracket c \rrbracket^{\pi \mathcal{I}} = c^{\mathcal{B}} = \pi(c^{\mathcal{A}}) = \pi(\llbracket c \rrbracket^{\mathcal{I}})$ .
- Sei  $x \in \mathsf{VAR}$ . **Behauptung:**  $\llbracket x \rrbracket^{\pi \mathcal{I}} = \pi(\llbracket x \rrbracket^{\mathcal{I}})$ .  
*Beweis:* Es gilt  $\llbracket x \rrbracket^{\pi \mathcal{I}} = (\pi\beta)(x) = \pi(\beta(x)) = \pi(\llbracket x \rrbracket^{\mathcal{I}})$ .

*Induktionsschritt:*

- Sei  $f \in \sigma$  ein Funktionssymbol, sei  $k := \text{ar}(f)$ , seien  $t_1, \dots, t_k$  beliebige  $\sigma$ -Terme.

**Induktionsannahme:** Für jedes  $i \in [k]$  gilt:  $\pi(\llbracket t_i \rrbracket^{\mathcal{I}}) = \llbracket t_i \rrbracket^{\pi \mathcal{I}}$ .

**Behauptung:** Es gilt:  $\llbracket f(t_1, \dots, t_k) \rrbracket^{\pi \mathcal{I}} = \pi(\llbracket f(t_1, \dots, t_k) \rrbracket^{\mathcal{I}})$ .

*Beweis:* Es gilt

$$\begin{array}{lcl}
 \llbracket f(t_1, \dots, t_k) \rrbracket^{\pi \mathcal{I}} & \stackrel{\text{Semantik}}{=} & f^{\mathcal{B}}(\llbracket t_1 \rrbracket^{\pi \mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\pi \mathcal{I}}) \\
 & \stackrel{\text{Ind.ann.}}{=} & f^{\mathcal{B}}(\pi(\llbracket t_1 \rrbracket^{\mathcal{I}}), \dots, \pi(\llbracket t_k \rrbracket^{\mathcal{I}})) \\
 & \stackrel{\pi: \mathcal{A} \cong \mathcal{B}}{=} & \pi(f^{\mathcal{A}}(\llbracket t_1 \rrbracket^{\mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\mathcal{I}})) \\
 & \stackrel{\text{Semantik}}{=} & \pi(\llbracket f(t_1, \dots, t_k) \rrbracket^{\mathcal{I}}).
 \end{array}$$

Dies beendet den Beweis von Teil (a) von Satz 3.24. □

Folie 215

Teil (b) des Isomorphielemmas beweisen wir per Induktion über den Aufbau von Formeln. Prinzipiell sind solche Induktionsbeweise wie folgt aufgebaut.

Folie 216

### Beweise per Induktion über den Aufbau von Formeln

Schematisch sieht der Beweis einer Aussage  $\mathbb{A}(\varphi)$  für alle FO[ $\sigma$ ]-Formeln  $\varphi$  wie folgt aus:

*Induktionsanfang:*

- Beweise, dass für alle  $\sigma$ -Terme  $t_1, t_2 \in \mathbb{T}_\sigma$  die Aussage  $\mathbb{A}(t_1=t_2)$  gilt.
- Beweise, dass für alle Relationssymbole  $R \in \sigma$ , für  $k := \text{ar}(R)$  und für alle  $\sigma$ -Terme  $t_1, \dots, t_k \in \mathbb{T}_\sigma$  die Aussage  $\mathbb{A}(R(t_1, \dots, t_k))$  gilt

Folie 217

*Induktionsschritt:*

Seien  $\varphi$  und  $\psi$  beliebige FO[ $\sigma$ ]-Formeln. Die *Induktionsannahme* besagt, dass die Aussagen  $\mathbb{A}(\varphi)$  und  $\mathbb{A}(\psi)$  gelten.

Im Induktionsschritt muss dann gezeigt werden, dass

- für jede Variable  $x \in \text{VAR}$  die Aussage  $\mathbb{A}(\exists x \varphi)$  gilt,
- für jede Variable  $x \in \text{VAR}$  die Aussage  $\mathbb{A}(\forall x \varphi)$  gilt,
- die Aussage  $\mathbb{A}(\neg \varphi)$  gilt,
- die Aussage  $\mathbb{A}((\varphi \wedge \psi))$  gilt,
- die Aussage  $\mathbb{A}((\varphi \vee \psi))$  gilt,

- die Aussage  $\mathbb{A}((\varphi \rightarrow \psi))$  gilt.

Mit dieser Vorgehensweise beweisen wir nun Teil (b) des Isomorphielemmas.

**Beweis von Teil (b) von Satz 3.24 (Isomorphielemma).**

Per Induktion über den Aufbau von Formeln. Die Aussage  $\mathbb{A}(\varphi)$ , die wir für alle FO[ $\sigma$ ]-Formeln  $\varphi$  beweisen wollen, besagt Folgendes:

Für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  
 $\pi\mathcal{I} \models \varphi \iff \mathcal{I} \models \varphi$ .

*Induktionsanfang:*

- Seien  $t_1, t_2 \in \mathbb{T}_\sigma$  zwei  $\sigma$ -Terme.

**Behauptung:** Für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  
 $\pi\mathcal{I} \models t_1=t_2 \iff \mathcal{I} \models t_1=t_2$ .

*Beweis:* Sei  $\beta$  eine beliebige Belegung in  $\mathcal{A}$  und sei  $\mathcal{I} := (\mathcal{A}, \beta)$ . Gemäß Teil (a) des Isomorphielemmas gilt für jedes  $i \in \{1, 2\}$ , dass  $\llbracket t_i \rrbracket^{\pi\mathcal{I}} = \pi(\llbracket t_i \rrbracket^{\mathcal{I}})$ . Somit gilt:

$$\begin{aligned} \pi\mathcal{I} \models t_1=t_2 &\stackrel{\text{Semantik}}{\iff} \llbracket t_1 \rrbracket^{\pi\mathcal{I}} = \llbracket t_2 \rrbracket^{\pi\mathcal{I}} \\ &\stackrel{(a)}{\iff} \pi(\llbracket t_1 \rrbracket^{\mathcal{I}}) = \pi(\llbracket t_2 \rrbracket^{\mathcal{I}}) \\ &\stackrel{\pi \text{ bijektiv}}{\iff} \llbracket t_1 \rrbracket^{\mathcal{I}} = \llbracket t_2 \rrbracket^{\mathcal{I}} \\ &\stackrel{\text{Semantik}}{\iff} \mathcal{I} \models t_1=t_2. \end{aligned}$$

- Sei  $R \in \sigma$  ein Relationssymbol, sei  $k = \text{ar}(R)$  und seien  $t_1, \dots, t_k \in \mathbb{T}_\sigma$ .

**Behauptung:** Für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  
 $\pi\mathcal{I} \models R(t_1, \dots, t_k) \iff \mathcal{I} \models R(t_1, \dots, t_k)$ .

*Beweis:* Sei  $\beta$  eine beliebige Belegung in  $\mathcal{A}$  und sei  $\mathcal{I} := (\mathcal{A}, \beta)$ . Gemäß Teil (a) des Isomorphielemmas gilt für jedes  $i \in [k]$ , dass  $\llbracket t_i \rrbracket^{\pi\mathcal{I}} = \pi(\llbracket t_i \rrbracket^{\mathcal{I}})$ . Somit gilt:

$$\begin{aligned} \pi\mathcal{I} \models R(t_1, \dots, t_k) &\stackrel{\text{Semantik}}{\iff} (\llbracket t_1 \rrbracket^{\pi\mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\pi\mathcal{I}}) \in R^{\mathcal{B}} \\ &\stackrel{(a)}{\iff} (\pi(\llbracket t_1 \rrbracket^{\mathcal{I}}), \dots, \pi(\llbracket t_k \rrbracket^{\mathcal{I}})) \in R^{\mathcal{B}} \\ &\stackrel{\pi: \mathcal{A} \cong \mathcal{B}}{\iff} (\llbracket t_1 \rrbracket^{\mathcal{I}}, \dots, \llbracket t_k \rrbracket^{\mathcal{I}}) \in R^{\mathcal{A}} \\ &\stackrel{\text{Semantik}}{\iff} \mathcal{I} \models R(t_1, \dots, t_k). \end{aligned}$$

*Induktionsschritt:*

Seien  $\varphi$  und  $\psi$  beliebige FO[ $\sigma$ ]-Formeln.

**Induktionsannahme:** Für jede Belegung  $\beta'$  in  $\mathcal{A}$ , für  $\mathcal{I}' := (\mathcal{A}, \beta')$  und für jede Formel  $\chi \in \{\varphi, \psi\}$  gilt:  $\pi\mathcal{I}' \models \chi \iff \mathcal{I}' \models \chi$ .

- **Behauptung 1:** Für jede Variable  $x \in \text{VAR}$ , für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  $\pi\mathcal{I} \models \exists x \varphi \iff \mathcal{I} \models \exists x \varphi$ .

*Beweis:* Sei  $x \in \text{VAR}$  eine beliebige Variable, und sei  $\beta$  eine beliebige Belegung in  $\mathcal{A}$ .

Wir nutzen, dass gemäß Lemma 3.23 für jedes  $a \in A$ , die Belegung  $\beta' := \beta \frac{a}{x}$ , die Interpretation  $\mathcal{I}' = \mathcal{I} \frac{a}{x} = (\mathcal{A}, \beta')$  und den Wert  $b := \pi(a)$  gilt:  $\pi\mathcal{I}' = (\pi\mathcal{I}) \frac{b}{x}$ .

Gemäß Induktionsannahme gilt:  $\pi\mathcal{I}' \models \varphi \iff \mathcal{I}' \models \varphi$ .

Somit gilt für alle  $a \in A$  und für  $b := \pi(a)$ , dass

$$(\pi\mathcal{I}) \frac{b}{x} \models \varphi \iff \mathcal{I} \frac{a}{x} \models \varphi. \quad (3.1)$$

Es folgt:

$$\begin{array}{lcl} \mathcal{I} \models \exists x \varphi & \stackrel{\text{Semantik}}{\iff} & \text{es gibt (mind.) ein } a \in A, \text{ so dass } \mathcal{I} \frac{a}{x} \models \varphi \\ (3.1) \text{ mit } b=\pi(a) & \stackrel{\text{mit } b=\pi(a)}{\iff} & \text{es gibt (mind.) ein } a \in A, \text{ so dass } (\pi\mathcal{I}) \frac{\pi(a)}{x} \models \varphi \\ \pi \text{ bijektiv} & \stackrel{\pi \text{ bijektiv}}{\iff} & \text{es gibt (mind.) ein } b \in B, \text{ so dass } (\pi\mathcal{I}) \frac{b}{x} \models \varphi \\ \text{Semantik} & \stackrel{\text{Semantik}}{\iff} & \pi\mathcal{I} \models \exists x \varphi. \end{array}$$

- **Behauptung 2:** Für jede Variable  $x \in \text{VAR}$ , für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  $\pi\mathcal{I} \models \forall x \varphi \iff \mathcal{I} \models \forall x \varphi$ .

*Beweis:* Der Beweis folgt analog zum Beweis der Behauptung 1:

Sei  $x \in \text{VAR}$  eine beliebige Variable, und sei  $\beta$  eine beliebige Belegung in  $\mathcal{A}$ . Dann gilt:

$$\begin{array}{lcl} \mathcal{I} \models \forall x \varphi & \stackrel{\text{Semantik}}{\iff} & \text{für jedes } a \in A \text{ gilt: } \mathcal{I} \frac{a}{x} \models \varphi \\ (3.1) \text{ mit } b=\pi(a) & \stackrel{\text{mit } b=\pi(a)}{\iff} & \text{für jedes } a \in A \text{ gilt: } (\pi\mathcal{I}) \frac{\pi(a)}{x} \models \varphi \\ \pi \text{ bijektiv} & \stackrel{\pi \text{ bijektiv}}{\iff} & \text{für jedes } b \in B \text{ gilt: } (\pi\mathcal{I}) \frac{b}{x} \models \varphi \\ \text{Semantik} & \stackrel{\text{Semantik}}{\iff} & \pi\mathcal{I} \models \forall x \varphi. \end{array}$$

- **Behauptung 3:** Für jede Belegung  $\beta$  in  $\mathcal{A}$  und für  $\mathcal{I} := (\mathcal{A}, \beta)$  gilt:  
 $\pi\mathcal{I} \models \neg\varphi \iff \mathcal{I} \models \neg\varphi.$

*Beweis:* Die Behauptung folgt direkt aus der Induktionsannahme und der Definition der Semantik von „ $\neg$ “.

- **Behauptung 4:** Für jede Belegung  $\beta$  in  $\mathcal{A}$ , für  $\mathcal{I} := (\mathcal{A}, \beta)$  und für jedes  $*$   $\in \{\wedge, \vee, \rightarrow\}$  gilt:  $\pi\mathcal{I} \models (\varphi * \psi) \iff \mathcal{I} \models (\varphi * \psi).$

*Beweis:* Die Behauptung folgt direkt aus der Induktionsannahme und der Definition der Semantik von „ $\wedge$ “, „ $\vee$ “ und „ $\rightarrow$ “.

Dies beendet den Beweis von Teil (b) von Satz 3.24. □

### Das Koinzidenzlemma

Folie 218

Ähnlich wie für die Aussagenlogik gilt auch für die Logik erster Stufe ein *Koinzidenzlemma*, das besagt, dass der Wert  $\llbracket t \rrbracket^{\mathcal{I}}$  eines Terms  $t$  bzw. der Wert  $\llbracket \varphi \rrbracket^{\mathcal{I}}$  einer Formel  $\varphi$  nur abhängt von

- denjenigen Bestandteilen von  $\mathcal{A}$ , die explizit in  $t$  bzw.  $\varphi$  vorkommen, und
- den Belegungen  $\beta(x)$  derjenigen Variablen  $x$ , die in  $t$  vorkommen bzw. die in  $\varphi$  vorkommen und *nicht im Wirkungsbereich eines Quantors* stehen.

Um diese Aussage präzise zu formulieren, sind folgende Begriffe nützlich.

Folie 219

### Definition 3.25.

(a) Ist  $\xi$  ein Term oder eine Formel der Logik erster Stufe, so schreiben wir

- $\sigma(\xi)$ , um die Menge aller Relations-, Funktions- und Konstantensymbole zu bezeichnen, die in  $\xi$  vorkommen,
- $\text{var}(\xi)$ , um die Menge aller in  $\xi$  vorkommenden Variablen zu bezeichnen.



- (b) Ist  $\varphi$  eine Formel und  $x$  eine Variable, so heißt jedes Vorkommen von  $x$  in einer Subformel von  $\varphi$ , die von der Form  $\exists x\psi$  oder  $\forall x\psi$  ist, *gebunden*. Jedes andere Vorkommen von  $x$  in  $\varphi$  heißt *frei*.

*Beispiel:*

$$\varphi := ( f(v_0, c)=v_3 \wedge \exists v_0 f(v_0, v_1)=c )$$

Das erste Vorkommen von  $v_0$  in  $\varphi$  ist frei, das zweite und dritte Vorkommen von  $v_0$  in  $\varphi$  ist gebunden. Die Vorkommen von  $v_1$  und  $v_3$  in  $\varphi$  sind frei.

Folie 220

## Freie Variablen

**Definition 3.26.** Die Menge  $\text{frei}(\varphi)$  aller *freien Variablen* einer Formel  $\varphi$  besteht aus allen Variablen, die mindestens ein freies Vorkommen in  $\varphi$  haben.

Die Menge  $\text{frei}(\varphi)$  lässt sich rekursiv über den Aufbau von Formeln wie folgt definieren:

$$\begin{aligned} \text{frei}(R(t_1, \dots, t_k)) &:= \text{var}(t_1) \cup \dots \cup \text{var}(t_k) \\ \text{frei}(t_1=t_2) &:= \text{var}(t_1) \cup \text{var}(t_2) \\ \text{frei}(\neg\varphi) &:= \text{frei}(\varphi) \\ \text{frei}((\varphi * \psi)) &:= \text{frei}(\varphi) \cup \text{frei}(\psi) \quad \text{für alle } * \in \{\wedge, \vee, \rightarrow\} \\ \text{frei}(\exists x \varphi) &:= \text{frei}(\forall x \varphi) := \text{frei}(\varphi) \setminus \{x\}. \end{aligned}$$

*Beispiele:*

- $\text{frei}(f(v_0, c)=v_3) = \{v_0, v_3\}$
- $\text{frei}(\exists v_0 f(v_0, v_1)=c) = \{v_1\}$
- $\text{frei}(( f(v_0, c)=v_3 \wedge \exists v_0 f(v_0, v_1)=c )) = \{v_0, v_3, v_1\}$

Folie 221

## Das Koinzidenzlemma

**Satz 3.27** (Koinzidenzlemma für Terme).

Sei  $\mathcal{I}_1 = (\mathcal{A}_1, \beta_1)$  eine  $\sigma_1$ -Interpretation und sei  $\mathcal{I}_2 = (\mathcal{A}_2, \beta_2)$  eine  $\sigma_2$ -Interpretation, wobei  $\sigma_1$  und  $\sigma_2$  Signaturen sind.

Sei  $t \in \mathbb{T}$  ein Term mit  $\sigma(t) \subseteq \sigma_1 \cap \sigma_2$ , so dass gilt:

1.  $\mathcal{A}_1|_{\sigma(t)} = \mathcal{A}_2|_{\sigma(t)}$   
(d.h., die  $\sigma(t)$ -Redukte von  $\mathcal{A}_1$  und  $\mathcal{A}_2$  sind identisch), und
2.  $\beta_1(x) = \beta_2(x)$ , für alle  $x \in \text{var}(t)$ .

Dann gilt:  $\llbracket t \rrbracket^{\mathcal{I}_1} = \llbracket t \rrbracket^{\mathcal{I}_2}$ .

*Beweis:* Per Induktion über den Aufbau von Termen. Details: Übung.  $\square$

**Satz 3.28** (Koinzidenzlemma für FO-Formeln).

Sei  $\mathcal{I}_1 = (\mathcal{A}_1, \beta_1)$  eine  $\sigma_1$ -Interpretation und sei  $\mathcal{I}_2 = (\mathcal{A}_2, \beta_2)$  eine  $\sigma_2$ -Interpretation, wobei  $\sigma_1$  und  $\sigma_2$  Signaturen seien.

Sei  $\varphi \in \text{FO}$  eine Formel der Logik erster Stufe mit  $\sigma(\varphi) \subseteq \sigma_1 \cap \sigma_2$ , so dass gilt:

1.  $\mathcal{A}_1|_{\sigma(\varphi)} = \mathcal{A}_2|_{\sigma(\varphi)}$ , und
2.  $\beta_1(x) = \beta_2(x)$ , für alle  $x \in \text{frei}(\varphi)$ .

Dann gilt:  $\mathcal{I}_1 \models \varphi \iff \mathcal{I}_2 \models \varphi$ .

*Beweis:* Per Induktion über den Aufbau von Formeln. Details: Übung.  $\square$

## Notation für Terme

- Für einen Term  $t \in \mathbb{T}_\sigma$  schreiben wir  $t(x_1, \dots, x_n)$ , um anzudeuten, dass  $\text{var}(t) \subseteq \{x_1, \dots, x_n\}$ .
- Sei  $\mathcal{A}$  eine  $\sigma$ -Struktur und seien  $a_1, \dots, a_n \in A$  Elemente des Universums von  $\mathcal{A}$ .

Auf Grund des Koinzidenzlemmas gilt

$$\llbracket t \rrbracket^{(\mathcal{A}, \beta)} = \llbracket t \rrbracket^{(\mathcal{A}, \beta')}$$

für alle Belegungen  $\beta, \beta' : \text{VAR} \rightarrow A$ , so dass  $\beta(x_i) = a_i = \beta'(x_i)$  für alle  $i \in [n]$  gilt. Wir schreiben oft

$$t^A[a_1, \dots, a_n],$$

um das Element  $\llbracket t \rrbracket^{(\mathcal{A}, \beta)}$  zu bezeichnen.

- Für Terme  $t \in \mathsf{T}_\sigma$ , in denen keine Variable vorkommt, d.h.  $\text{var}(t) = \emptyset$  (so genannte *Grundterme*), schreiben wir einfach  $t^A$ .

Folie 223

### Notation für Formeln

- Für eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  schreiben wir  $\varphi(x_1, \dots, x_n)$ , um anzudeuten, dass  $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_n\}$ .
- Ist  $\mathcal{A}$  eine  $\sigma$ -Struktur und sind  $a_1, \dots, a_n \in A$ , so schreiben wir

$$\mathcal{A} \models \varphi[a_1, \dots, a_n]$$

wenn  $(\mathcal{A}, \beta) \models \varphi$  für eine Belegung  $\beta : \text{VAR} \rightarrow A$  mit  $\beta(x_i) = a_i$  für alle  $i \in [n]$  gilt. Auf Grund des Koinzidenzlemmas gilt dann auch für alle Belegungen  $\beta' : \text{VAR} \rightarrow A$  mit  $\beta'(x_i) = a_i$  für alle  $i \in [n]$ , dass  $(\mathcal{A}, \beta') \models \varphi$ .

### Sätze der Logik erster Stufe

Folie 224

**Definition 3.29.** Sei  $\sigma$  eine Signatur.

- Ein  $\text{FO}[\sigma]$ -Satz (kurz: *Satz*) ist eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  mit  $\text{frei}(\varphi) = \emptyset$ .
- Wir schreiben  $\mathsf{S}_\sigma$ , um die Menge aller  $\text{FO}[\sigma]$ -Sätze zu bezeichnen und setzen

$$\mathsf{S} := \bigcup_{\sigma \text{ Signatur}} \mathsf{S}_\sigma.$$

- Für einen  $\text{FO}[\sigma]$ -Satz  $\varphi$  und eine  $\sigma$ -Struktur  $\mathcal{A}$  schreiben wir  $\mathcal{A} \models \varphi$ , um auszudrücken, dass  $(\mathcal{A}, \beta) \models \varphi$  für eine (und gemäß Koinzidenzlemma daher für jede) Belegung  $\beta$  in  $\mathcal{A}$  gilt.

- (d) Für eine Menge  $\Phi \subseteq S_\sigma$  von FO[ $\sigma$ ]-Sätzen schreiben wir  $\mathcal{A} \models \Phi$ , falls  $\mathcal{A} \models \varphi$  für jedes  $\varphi \in \Phi$  gilt.

Als direkte Folgerung aus dem Isomorphielemma erhalten wir, dass für isomorphe  $\sigma$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  und für alle FO[ $\sigma$ ]-Sätze  $\varphi$  gilt:

$$\mathcal{A} \models \varphi \iff \mathcal{B} \models \varphi.$$

Folie 225

### Modellklassen und Definierbarkeit

**Definition 3.30.** Sei  $\sigma$  eine Signatur und sei  $\Phi \subseteq S_\sigma$  (d.h.  $\Phi$  ist eine Menge von FO[ $\sigma$ ]-Sätzen).

- (a) Die *Modellklasse* von  $\Phi$  ist die Klasse  $\text{MOD}_\sigma(\Phi)$  aller  $\sigma$ -Strukturen  $\mathcal{A}$  für die gilt:  $\mathcal{A} \models \Phi$ .
- (b) Für eine Klasse  $\mathcal{C}$  von  $\sigma$ -Strukturen sagen wir

$\Phi$  *definiert* (oder *axiomatisiert*)  $\mathcal{C}$ ,

falls  $\mathcal{C} = \text{MOD}_\sigma(\Phi)$ .

- (c) Für einen FO[ $\sigma$ ]-Satz  $\varphi$  setzen wir  $\text{MOD}_\sigma(\varphi) := \text{MOD}_\sigma(\{\varphi\})$  und sagen, dass  $\varphi$  die Klasse  $\mathcal{C} := \text{MOD}_\sigma(\varphi)$  definiert (bzw. axiomatisiert).

Als direkte Folgerung aus dem Isomorphielemma erhalten wir:

**Korollar 3.31.** Für jede Signatur  $\sigma$  und jedes  $\Phi \subseteq S_\sigma$  ist  $\text{MOD}_\sigma(\Phi)$  unter Isomorphie abgeschlossen. D.h. für isomorphe  $\sigma$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  gilt:

$$\mathcal{A} \in \text{MOD}_\sigma(\Phi) \iff \mathcal{B} \in \text{MOD}_\sigma(\Phi).$$

*Beweis:* klar. □

### 3.5 Beispiele für Formeln der Logik erster Stufe in verschiedenen Anwendungsbereichen

Folie 226

#### Notation

- Ab jetzt verwenden wir für die Logik erster Stufe ähnliche *Klammerkonventionen* wie bei der Aussagenlogik.
- Für gewisse zweistellige Funktionssymbole wie  $+$ ,  $\cdot$  und zweistellige Relationssymbole wie  $\leq$  verwenden wir *Infix-* statt Präfixnotation. Dabei setzen wir auf natürliche Weise Klammern, um die eindeutige Lesbarkeit zu gewährleisten.
- Wir schreiben  $x < y$  als Abkürzung für die Formel  $(x \leq y \wedge \neg x=y)$ .

Folie 227

#### Ordnungen

**Beispiel 3.32.** Wir betrachten Strukturen und Formeln über der Signatur  $\sigma := \{\leq\}$ .

*Zur Erinnerung:* Eine  $\sigma$ -Struktur  $\mathcal{A} = (A, \leq^{\mathcal{A}})$  ist eine *lineare Ordnung*, falls gilt:

(1)  $\leq^{\mathcal{A}}$  ist *reflexiv*,

- d.h. für alle  $a \in A$  gilt:  $a \leq^{\mathcal{A}} a$
- d.h.  $\mathcal{A} \models \varphi_{\text{refl}}$ , wobei

$$\varphi_{\text{refl}} := \forall x \ x \leq x$$

(2)  $\leq^{\mathcal{A}}$  ist *transitiv*,

- d.h. für alle  $a, b, c \in A$  gilt: Wenn  $a \leq^{\mathcal{A}} b$  und  $b \leq^{\mathcal{A}} c$ , dann auch  $a \leq^{\mathcal{A}} c$
- d.h.  $\mathcal{A} \models \varphi_{\text{trans}}$ , wobei

$$\varphi_{\text{trans}} := \forall x \forall y \forall z \left( (x \leq y \wedge y \leq z) \rightarrow x \leq z \right)$$

Folie 228

(3)  $\leq^A$  ist *antisymmetrisch*,

- d.h. für alle  $a, b \in A$  mit  $a \neq b$  gilt: Wenn  $a \leq^A b$ , dann  $b \not\leq^A a$
- d.h.  $\mathcal{A} \models \varphi_{antisym}$ , wobei

$$\varphi_{antisym} := \forall x \forall y \left( \neg x = y \rightarrow (x \leq y \rightarrow \neg y \leq x) \right)$$

(4)  $\leq^A$  ist *konnekt*,

- d.h. für alle  $a, b \in A$  gilt:  $a \leq^A b$  oder  $b \leq^A a$  oder  $a = b$
- d.h.  $\mathcal{A} \models \varphi_{konnekt}$ , wobei

$$\varphi_{konnekt} := \forall x \forall y \left( x \leq y \vee y \leq x \vee x = y \right)$$

Insgesamt gilt für jede  $\{\leq\}$ -Struktur  $\mathcal{A} = (A, \leq^A)$ :

$\mathcal{A} = (A, \leq^A)$  ist eine lineare Ordnung  $\iff \mathcal{A} \models \varphi_{lin.Ord}$ , wobei

$$\varphi_{lin.Ord} := \varphi_{refl} \wedge \varphi_{antisym} \wedge \varphi_{trans} \wedge \varphi_{konnekt}$$

Der FO[ $\sigma$ ]-Satz  $\varphi_{lin.Ord}$  definiert (bzw. axiomatisiert) also die Klasse aller linearen Ordnungen.

Folie 229

## Arithmetik

**Beispiel 3.33.** Wir betrachten Formeln über der Signatur  $\sigma := \{+, \cdot, \leq, \underline{0}, \underline{1}\}$  und ihre Bedeutung im *Standardmodell*  $\mathcal{A}_{\mathbb{N}}$  der *Arithmetik*.

- *Gesucht:* Eine FO[ $\sigma$ ]-Formel  $\varphi_-(x, y, z)$ , die besagt „ $x - y = z$ “.

*Präzise:* Für alle  $a, b, c \in \mathbb{N}$  soll gelten:

$$\mathcal{A}_{\mathbb{N}} \models \varphi_-[a, b, c] \iff a - b = c.$$

*Lösung:*

$$\varphi_-(x, y, z) := x = z + y$$

- *Gesucht:* Eine FO[ $\sigma$ ]-Formel  $\varphi_|(x, y)$ , die besagt „ $x$  teilt  $y$ “.

*Präzise:* Für alle  $a, b \in \mathbb{N}$  soll gelten:

$$\mathcal{A}_{\mathbb{N}} \models \varphi_|[a, b] \iff \text{es gibt ein } c \in \mathbb{N}, \text{ so dass } a \cdot c = b.$$

*Lösung:*

$$\varphi_|(x, y) := \exists z \ x \cdot z = y$$

- *Gesucht:* Eine FO[ $\sigma$ ]-Formel  $\varphi_{\equiv}(x, y, z)$ , die besagt „ $x \equiv y \pmod{z}$ “.  
*Präzise:* Für alle  $a, b, c \in \mathbb{N}$  soll gelten:

$$\mathcal{A}_{\mathbb{N}} \models \varphi_{\equiv}[a, b, c] \iff a \equiv b \pmod{c} \quad \text{d.h.} \quad c \mid |a - b|$$

*Lösung:*

$$\varphi_{\equiv}(x, y, z) := \exists w \left( \underbrace{(\varphi_{-}(x, y, w) \vee \varphi_{-}(y, x, w))}_{\text{„}w = |x - y|\text{“}} \wedge \underbrace{\varphi_{\mid}(z, w)}_{\text{„}z \mid w\text{“}} \right)$$

- *Gesucht:* Eine FO[ $\sigma$ ]-Formel  $\varphi_{\text{prim}}(x)$ , die besagt „ $x$  ist eine Primzahl“.  
*Präzise:* Für alle  $a \in \mathbb{N}$  soll gelten:

$$\mathcal{A}_{\mathbb{N}} \models \varphi_{\text{prim}}[a] \iff a \text{ ist eine Primzahl}$$

d.h.  $a \geq 2$  und  $a$  ist nur durch sich selbst und durch 1 teilbar.

*Lösung:*

$$\varphi_{\text{prim}}(x) := \underbrace{\underline{1} + \underline{1} \leq x}_{\text{„}x \geq 2\text{“}} \wedge \forall z \left( \underbrace{\varphi_{\mid}(z, x)}_{\text{„}z \mid x\text{“}} \rightarrow (z = x \vee z = \underline{1}) \right)$$

- *Gesucht:* Ein FO[ $\sigma$ ]-Satz  $\varphi_{\infty}$ , der in  $\mathcal{A}_{\mathbb{N}}$  besagt

„Es gibt unendlich viele Primzahlen“.

*Lösung:*

$$\varphi_{\infty} := \forall y \exists x \left( y \leq x \wedge \varphi_{\text{prim}}(x) \right)$$

In  $\mathcal{A}_{\mathbb{N}}$  besagt dieser Satz, dass es für jede natürliche Zahl  $b$  eine natürliche Zahl  $a \geq b$  gibt, die eine Primzahl ist.

## Worte

**Beispiel 3.34.** Wir betrachten das Alphabet  $\Sigma := \{a, b\}$  und die Signatur  $\sigma_\Sigma = \{\leq, P_a, P_b\}$ .

*Zur Erinnerung:* Wir repräsentieren ein nicht-leeres Wort  $w \in \Sigma^*$  durch die  $\sigma_\Sigma$ -Struktur  $\mathcal{A}_w$ , deren Universum aus der Menge  $\{1, \dots, |w|\}$  aller Positionen in  $w$  besteht, und bei der  $P_a^{\mathcal{A}_w}$  (bzw.  $P_b^{\mathcal{A}_w}$ ) aus allen Positionen besteht, an denen der Buchstabe  $a$  (bzw.  $b$ ) steht.

*Gesucht:* Ein FO[ $\sigma_\Sigma$ ]-Satz  $\varphi$ , so dass für jedes nicht-leere Wort  $w \in \Sigma^*$  gilt:

$$\mathcal{A}_w \models \varphi \iff w \text{ ist von der Form } a^*b^*.$$

*Lösung:* Wir konstruieren eine Formel  $\varphi$ , die besagt, dass es eine Position  $x$  gibt, so dass alle Positionen links von  $x$  den Buchstaben  $a$  tragen und alle Positionen rechts von  $x$  den Buchstaben  $b$  tragen. Dies wird durch folgenden FO[ $\sigma_\Sigma$ ]-Satz realisiert:

$$\varphi := \exists x \forall y \left( (y < x \rightarrow P_a(y)) \wedge (x < y \rightarrow P_b(y)) \right)$$

Wie bereits vereinbart, schreiben wir hier „ $x < y$ “ als Abkürzung für die Formel  $(x \leq y \wedge \neg x = y)$ .

## 3.6 Logik und Datenbanken

Folie 233

### Datenbanken

*Zur Erinnerung:* Wir repräsentieren eine Kinodatenbank, die Informationen über Kinos, Filme und das aktuelle Programm enthält, durch eine Struktur über der Signatur  $\sigma_{\text{KINO}} :=$

$$\{ R_{\text{Kino}}/4, R_{\text{Film}}/3, R_{\text{Prog}}/3 \} \cup \{ 'c' : c \in \text{ASCII}^* \}$$

und können so z.B. die folgende Kinodatenbank als  $\sigma_{\text{KINO}}$ -Struktur  $\mathcal{D}$  auffassen, deren Universum  $D$  aus der Menge aller Worte über dem ASCII-Alphabet besteht.

Folie 234



## Beispiel: Eine Kinodatenbank

<i>Kino</i>			
Name	Adresse	Stadtteil	Telefonnummer
Babylon	Dresdner Str. 126	Kreuzberg	030 61 60 96 93
Casablanca	Friedenstr. 12-13	Adlershof	030 67 75 75 2
Filmtheater am Friedrichshain	Bötzowstr. 1-5	Prenzlauer Berg	030 42 84 51 88
Kino International	Karl-Marx-Allee 33	Mitte	030 24 75 60 11
Movimento	Kotbusser Damm 22	Kreuzberg	030 692 47 85
Urania	An der Urania 17	Schöneberg	030 21 89 09 1

<i>Film</i>		
Name	Regisseur	Schauspieler
Alien	Ridley Scott	Sigourney Weaver
Blade Runner	Ridley Scott	Harrison Ford
Blade Runner	Ridley Scott	Sean Young
Brazil	Terry Gilliam	Jonathan Pryce
Brazil	Terry Gilliam	Kim Greist
Casablanca	Michael Curtiz	Humphrey Bogart
Casablanca	Michael Curtiz	Ingrid Bergmann
Gravity	Alfonso Cuaron	Sandra Bullock
Gravity	Alfonso Cuaron	George Clooney
Monuments Men	George Clooney	George Clooney
Monuments Men	George Clooney	Matt Damon
Resident Evil	Paul Anderson	Milla Jovovich
Terminator	James Cameron	Arnold Schwarzenegger
Terminator	James Cameron	Linda Hamilton
Terminator	James Cameron	Michael Biehn
...	...	...

Folie 235

<i>Programm</i>		
Kino	Film	Zeit
Babylon	Casablanca	17:30
Babylon	Gravity	20:15
Casablanca	Blade Runner	15:30
Casablanca	Alien	18:15
Casablanca	Blade Runner	20:30
Casablanca	Resident Evil	20:30
Filmtheater am Friedrichshain	Resident Evil	20:00
Filmtheater am Friedrichshain	Resident Evil	21:30
Filmtheater am Friedrichshain	Resident Evil	23:00
Kino International	Casablanca	18:00
Kino International	Brazil	20:00
Kino International	Brazil	22:00
Movimento	Gravity	17:00
Movimento	Gravity	19:30
Movimento	Alien	22:00
Urania	Monuments Men	17:00
Urania	Monuments Men	20:00

Folie 236

## Die Kinodatenbank als Struktur

*Signatur:*  $\sigma_{\text{KINO}} := \{ R_{\text{Kino}}/4, R_{\text{Film}}/3, R_{\text{Prog}}/3 \} \cup \{ 'c' : c \in \text{ASCII}^* \}$

Die Kinodatenbank wird dargestellt als  $\sigma_{\text{KINO}}$ -Struktur  $\mathcal{D}$ .

*Universum:*

$D := \text{ASCII}^* \supseteq \{ \text{Babylon, Dresdner Str. 126, Kreuzberg, 030 61 60 96 93, Casablanca, \dots, 20:00} \}$ .

*Relationen:*

$R_{\text{Kino}}^{\mathcal{D}} := \{ (\text{Babylon, Dresdner Str. 126, Kreuzberg, 030 61 60 96 93}),$   
 $(\text{Casablanca, Friedenstr. 12-13, Adlershof, 030 67 75 75 2}),$   
 $(\text{Filmtheater am Friedrichshain, Böttzowstr. 1-5, Prenzlauer Berg, 030 42 84 51 88}),$   
 $(\text{Kino International, Karl-Marx-Allee 33, Mitte, 030 24 75 60 11}),$   
 $(\text{Movimiento, Kotbusser Damm 22, Kreuzberg, 030 692 47 85}),$   
 $(\text{Urania, An der Urania 17, Schöneberg, 030 21 89 09 1}) \}$

$R_{\text{Film}}^{\mathcal{D}} := \{ (\text{Alien, Ridley Scott, Sigourney Weaver}),$   
 $(\text{Blade Runner, Ridley Scott, Harrison Ford}), \dots \}$

$R_{\text{Prog}}^{\mathcal{D}} := \{ (\text{Babylon, Casablanca, 17:30}),$   
 $(\text{Babylon, Gravity, 20:15}), \dots \}$ .

*Konstanten:*  $'c^{\mathcal{D}} := c$ , für jedes  $c \in \text{ASCII}^*$ .

D.h.: jedes Konstantensymbol wird durch den zwischen den Hochkommas stehenden Text interpretiert.

Folie 237

**Beispiel 3.35.** (a) Die Anfrage

*„Gib die Titel aller Filme aus, die um 22:00 Uhr beginnen.“*

lässt sich durch folgende  $\text{FO}[\sigma_{\text{KINO}}]$ -Formel  $\varphi_1(x_T)$  beschreiben:

$$\varphi_1(x_T) := \exists x_K R_{\text{Prog}}(x_K, x_T, '22:00')$$

(b) Die Anfrage

*„Gib die Titel aller Filme aus, in denen George Clooney mitspielt oder Regie führt“*

lässt sich durch folgende  $\text{FO}[\sigma_{\text{KINO}}]$ -Formel beschreiben:  $\varphi_2(x_T) :=$

$$\exists x_R R_{\text{Film}}(x_T, x_R, 'George Clooney') \vee \exists x_S R_{\text{Film}}(x_T, 'George Clooney', x_S)$$

(c) Die Anfrage

„Gib Name und Stadtteil aller Kinos aus, in denen ein Film läuft, in dem George Clooney mitspielt oder Regie führt“

lässt sich durch folgende FO[ $\sigma_{\text{KINO}}$ ]-Formel beschreiben:

$\varphi_3(x_K, x_{St}) :=$

$$\begin{aligned} & \exists x_A \exists x_{Tel} R_{Kino}(x_K, x_A, x_{St}, x_{Tel}) \wedge \\ & \exists x_T \exists x_Z \left( R_{Prog}(x_K, x_T, x_Z) \wedge \right. \\ & \quad \left. (\exists x_R R_{Film}(x_T, x_R, \text{'George Clooney'}) \vee \exists x_S R_{Film}(x_T, \text{'George Clooney'}, x_S)) \right) \end{aligned}$$

Die erste Zeile der Formel stellt sicher, dass  $x_K$  ein Kino und  $x_S$  dessen Stadtteil ist; die Zeilen 2 und 3 stellen sicher, dass im Kino  $x_K$  ein Film läuft, in dem George Clooney mitspielt oder Regie führt.

## Eine andere Sichtweise auf die Semantik

- Anstatt *Wahrheitswerte in Interpretationen* definieren Formeln der Logik der ersten Stufe auch *Relationen in Strukturen*.
- Junktoren und Quantoren entsprechen dann algebraischen Operatoren auf Relationen.
- Diese Sichtweise ist insbesondere in der Datenbanktheorie wichtig und bildet die Grundlage effizienter Algorithmen zur Auswertung von Datenbankabfragen.

**Definition 3.36.** Sei  $\sigma$  eine Signatur, sei  $\varphi(x_1, \dots, x_n)$  eine FO[ $\sigma$ ]-Formel und sei  $\mathcal{A}$  eine  $\sigma$ -Struktur.

Die von  $\varphi(x_1, \dots, x_n)$  in  $\mathcal{A}$  definierte  $n$ -stellige Relation ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} := \{ (a_1, \dots, a_n) \in A^n : \mathcal{A} \models \varphi[a_1, \dots, a_n] \}.$$

*Vorsicht:* Die Relation  $\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$  hängt nicht nur von der Formel  $\varphi$  ab, sondern auch von dem Tupel  $(x_1, \dots, x_n) \in \text{VAR}^n$ .

**Beispiel 3.37.** Die FO[ $\sigma_{\text{KINO}}$ ]-Formeln  $\varphi_2(x_T)$  und  $\varphi_3(x_K, x_{St})$  aus Beispiel 3.35 definieren in unserer Beispiel-Datenbank  $\mathcal{D}$  die Relationen

$$\llbracket \varphi_2(x_T) \rrbracket^{\mathcal{D}} = \left\{ \begin{array}{l} (\text{Gravity}) , \\ (\text{Monuments Men}) \end{array} \right\}$$

und

$$\llbracket \varphi_3(x_K, x_{St}) \rrbracket^{\mathcal{D}} = \left\{ \begin{array}{l} (\text{Babylon, Kreuzberg}) , \\ (\text{Movimento, Kreuzberg}) , \\ (\text{Urania, Schöneberg}) \end{array} \right\}$$

Folie 241

## Ändern der Variablen

**Lemma 3.38.** Sei  $\sigma$  eine Signatur, sei  $\mathcal{A}$  eine  $\sigma$ -Struktur und sei  $\varphi(x_1, \dots, x_n) \in \text{FO}[\sigma]$ .

(a) Für jede Permutation<sup>1</sup>  $\pi$  von  $[n]$  ist

$$\llbracket \varphi(x_{\pi(1)}, \dots, x_{\pi(n)}) \rrbracket^{\mathcal{A}} = \left\{ (a_{\pi(1)}, \dots, a_{\pi(n)}) : (a_1, \dots, a_n) \in \llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \right\}.$$

(b) Für jede Variable  $y \in \text{VAR} \setminus \{x_1, \dots, x_n\}$  ist

$$\llbracket \varphi(x_1, \dots, x_n, y) \rrbracket^{\mathcal{A}} = \llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \times A.$$

(c) Falls  $x_n \notin \text{frei}(\varphi)$ , so ist

$$\llbracket \varphi(x_1, \dots, x_{n-1}) \rrbracket^{\mathcal{A}} = \left\{ (a_1, \dots, a_{n-1}) : \text{es gibt (mind.) ein } a \in A \text{ so dass } (a_1, \dots, a_{n-1}, a) \in \llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \right\}.$$

*Beweis.* (a) ist trivial. (b), (c) folgen direkt aus dem Koinzidenzlemma.  $\square$

Folie 242

<sup>1</sup>Eine *Permutation einer Menge*  $M$  ist eine bijektive Abbildung von  $M$  nach  $M$ .

## Rekursive Beschreibung von $\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$

**Beobachtung 3.39.** Ist  $\sigma$  eine Signatur und  $\mathcal{A}$  eine  $\sigma$ -Struktur, so können wir für FO[ $\sigma$ ]-Formeln  $\varphi$  und Variablen-tupel  $(x_1, \dots, x_n)$  mit  $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_n\}$  die Relation  $\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \subseteq A^n$  rekursiv wie folgt beschreiben:

- Falls  $\varphi$  von der Form  $t_1 = t_2$  für  $\sigma$ -Terme  $t_1, t_2$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \left\{ (a_1, \dots, a_n) \in A^n : \right. \\ \left. t_1^{\mathcal{A}}[a_1, \dots, a_n] = t_2^{\mathcal{A}}[a_1, \dots, a_n] \right\}$$

*Zur Erinnerung:* Für einen  $\sigma$ -Term  $t(x_1, \dots, x_n)$  schreiben wir  $t^{\mathcal{A}}[a_1, \dots, a_n]$  um das Element  $\llbracket t \rrbracket^{(\mathcal{A}, \beta)} \in A$  zu bezeichnen, wobei  $\beta$  eine Belegung mit  $\beta(x_i) = a_i$ , für alle  $i \in [n]$ , ist.

- Falls  $\varphi$  von der Form  $R(t_1, \dots, t_k)$  für ein  $R \in \sigma$ , für  $k := \text{ar}(R)$  und für  $\sigma$ -Terme  $t_1, \dots, t_k$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \left\{ (a_1, \dots, a_n) \in A^n : \right. \\ \left. (t_1^{\mathcal{A}}[a_1, \dots, a_n], \dots, t_k^{\mathcal{A}}[a_1, \dots, a_n]) \in R^{\mathcal{A}} \right\}$$

Folie 243

- Falls  $\varphi$  von der Form  $\neg\psi$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = A^n \setminus \llbracket \psi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$$

- Falls  $\varphi$  von der Form  $(\psi_1 \wedge \psi_2)$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \llbracket \psi_1(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \cap \llbracket \psi_2(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$$

- Falls  $\varphi$  von der Form  $(\psi_1 \vee \psi_2)$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \llbracket \psi_1(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \cup \llbracket \psi_2(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$$

- Falls  $\varphi$  von der Form  $(\psi_1 \rightarrow \psi_2)$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \llbracket \neg\psi_1(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} \cup \llbracket \psi_2(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$$

Folie 244

- Falls  $\varphi$  von der Form  $\exists y \psi$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \left\{ (a_1, \dots, a_n) \in A^n : \text{es gibt (mind.) ein } b \in A \text{ mit } (a_1, \dots, a_n, b) \in \llbracket \psi(x_1, \dots, x_n, y) \rrbracket^{\mathcal{A}} \right\}$$

Somit ist  $\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$  die *Projektion* von  $\llbracket \psi(x_1, \dots, x_n, y) \rrbracket^{\mathcal{A}}$  auf die ersten  $n$  Stellen.

- Falls  $\varphi$  von der Form  $\forall y \psi$  ist, so ist

$$\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}} = \left\{ (a_1, \dots, a_n) \in A^n : \text{für jedes } b \in A \text{ ist } (a_1, \dots, a_n, b) \in \llbracket \psi(x_1, \dots, x_n, y) \rrbracket^{\mathcal{A}} \right\}$$

Folie 245

### Das Auswertungsproblem für FO

*Eingabe:* Eine endliche Signatur  $\sigma$ ,  
 eine  $\sigma$ -Struktur  $\mathcal{A}$ , deren Universum  $A$  endlich ist,  
 eine FO[ $\sigma$ ]-Formel  $\varphi$ ,  
 eine Zahl  $n \in \mathbb{N}$  und  
 ein Variablentupel  $(x_1, \dots, x_n) \in \text{VAR}^n$ , so dass  $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_n\}$  ist.

*Aufgabe:* Berechne  $\llbracket \varphi(x_1, \dots, x_n) \rrbracket^{\mathcal{A}}$ .

Beobachtung 3.39 führt unmittelbar zu einem rekursiven Algorithmus, der das Auswertungsproblem für FO löst.

Eine Laufzeitanalyse zeigt, dass Folgendes gilt:

Folie 246

**Satz 3.40.** *Es gibt einen Algorithmus, der das Auswertungsproblem für FO bei Eingabe einer Signatur  $\sigma$ , einer  $\sigma$ -Struktur  $\mathcal{A}$ , einer FO[ $\sigma$ ]-Formel  $\varphi$ , einer Zahl  $n$  und eines Variablentupels  $(x_1, \dots, x_n)$  mit  $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_n\}$  in Zeit*

$$c \cdot (\|\varphi\| + \|\mathcal{A}\| + \|\varphi\| \cdot w \cdot \|\mathcal{A}\|^w)$$

*löst, wobei gilt:*

- $c \in \mathbb{N}_{\geq 1}$

- $\|\varphi\|$  ist die Länge von  $\varphi$ , aufgefasst als Wort über dem Alphabet  $A_{\text{FO}[\sigma]}$
- $w$  ist die maximale Anzahl freier Variablen in Subformeln von  $\varphi$  — die so genannte Breite (engl.: width) von  $\varphi$
- $\|\mathcal{A}\|$  ist ein Maß für die Größe einer geeigneten Repräsentation von  $\mathcal{A}$  als Eingabe für einen Algorithmus; präzise:

$$\|\mathcal{A}\| := |\sigma| + |A| + \sum_{R \in \sigma} |R^A| \cdot \text{ar}(R) + \sum_{f \in \sigma} |A|^{\text{ar}(f)} \cdot (\text{ar}(f) + 1)$$

(Hier ohne Beweis)

### 3.7 Äquivalenz von Formeln der Logik erster Stufe

Folie 247

#### Äquivalenz

**Definition 3.41.** Sei  $\sigma$  eine Signatur.

- (a) Zwei FO[ $\sigma$ ]-Formeln  $\varphi$  und  $\psi$  heißen *äquivalent* (kurz:  $\varphi \equiv \psi$ ), wenn für jede  $\sigma$ -Interpretation  $\mathcal{I}$  gilt:

$$\mathcal{I} \models \varphi \iff \mathcal{I} \models \psi.$$

- (b) Zwei Formelmengen  $\Phi, \Psi \subseteq \text{FO}[\sigma]$  heißen *äquivalent* (kurz:  $\Phi \equiv \Psi$ ), wenn für jede  $\sigma$ -Interpretation  $\mathcal{I}$  gilt:<sup>2</sup>

$$\mathcal{I} \models \Phi \iff \mathcal{I} \models \Psi.$$

Folie 248

#### Beispiel 3.42.

Welche der folgenden Formeln sind äquivalent, welche nicht?

- $\varphi_1 := \exists y E(x, y)$
- $\varphi_2 := \exists z E(x, z)$
- $\varphi_3 := \exists z E(y, z)$

---

<sup>2</sup>Zur Erinnerung:  $\mathcal{I} \models \Phi$  bedeutet, dass  $\mathcal{I} \models \varphi$  für jede Formel  $\varphi \in \Phi$  gilt.

*Antwort:*

(1)  $\varphi_1 \equiv \varphi_2$ , denn für jede  $\{E\}$ -Struktur  $\mathcal{A}$  und jede Belegung  $\beta : \text{VAR} \rightarrow A$  gilt für  $\mathcal{I} := (\mathcal{A}, \beta)$  Folgendes:  $\mathcal{I} \models \varphi_1 \iff$  es gibt ein Element  $a \in A$ , so dass es in  $E^{\mathcal{A}}$  eine Kante von  $\beta(x)$  zu  $a$  gibt (d.h.  $(\beta(x), a) \in E^{\mathcal{A}}) \iff \mathcal{I} \models \varphi_2$ .

(2)  $\varphi_2 \not\equiv \varphi_3$ , denn betrachte die  $\{E\}$ -Interpretation  $\mathcal{I} = (\mathcal{A}, \beta)$  mit  $A = \{1, 2\}$ ,  $E^{\mathcal{A}} = \{(1, 2)\}$ ,  $\beta(x) = 1$ ,  $\beta(y) = 2$  und  $\beta(v) = 1$  für alle  $v \in \text{VAR} \setminus \{x, y\}$ .

Für dieses  $\mathcal{I}$  gilt:  $\mathcal{I} \models \varphi_2$ , denn es gibt in  $\mathcal{A}$  einen Knoten, zu dem von  $\beta(x) = 1$  aus eine Kante führt — nämlich den Knoten 2. Andererseits gilt:  $\mathcal{I} \not\models \varphi_3$ , denn es gibt in  $\mathcal{A}$  keinen Knoten, zu dem von  $\beta(y) = 2$  aus eine Kante führt.

(3) Aus (1) und (2) und der Transitivität der Relation „ $\equiv$ “ folgt, dass  $\varphi_1 \not\equiv \varphi_3$ .

Folie 249

## Aussagenlogische Äquivalenzen

**Lemma 3.43.** *Ersetzt man in äquivalenten aussagenlogischen Formeln alle Aussagensymbole durch FO[ $\sigma$ ]-Formeln, so erhält man äquivalente FO[ $\sigma$ ]-Formeln.*

*Beispiel.* Aus der aussagenlogische Äquivalenz  $(X \rightarrow Y) \equiv \neg X \vee Y$  folgt, dass

$$(\varphi \rightarrow \psi) \equiv \neg\varphi \vee \psi$$

für alle FO[ $\sigma$ ]-Formeln  $\varphi$  und  $\psi$  gilt.

### **Beweis von Lemma 3.43:**

Seien  $\alpha, \alpha' \in \text{AL}$  zwei aussagenlogische Formeln.

Seien  $X_1, \dots, X_n$  die Aussagensymbole, die in  $\alpha$  oder  $\alpha'$  vorkommen.

Seien  $\varphi_1, \dots, \varphi_n \in \text{FO}[\sigma]$ .

Seien  $\alpha(\varphi_1, \dots, \varphi_n)$  bzw.  $\alpha'(\varphi_1, \dots, \varphi_n)$  die FO[ $\sigma$ ]-Formeln, die aus  $\alpha$  bzw.

$\alpha'$  entstehen, indem man jedes Vorkommen einer aussagenlogischen

Variablen  $X_i$  (für  $i \in [n]$ ) durch die FO[ $\sigma$ ]-Formel  $\varphi_i$  ersetzt.

Sei  $\mathcal{I}$  eine beliebige  $\sigma$ -Interpretation. Wir müssen zeigen, dass gilt:

$$\mathcal{I} \models \alpha(\varphi_1, \dots, \varphi_n) \iff \mathcal{I} \models \alpha'(\varphi_1, \dots, \varphi_n).$$



Sei  $\tilde{\mathcal{I}}$  eine aussagenlogische Interpretation mit  $\tilde{\mathcal{I}}(X_i) = \llbracket \varphi_i \rrbracket^{\tilde{\mathcal{I}}}$  jedes  $i \in [n]$ . Per Induktion nach dem Aufbau von  $\alpha$  lässt sich leicht zeigen (Details: Übung), dass Folgendes gilt:

$$\mathcal{I} \models \alpha(\varphi_1, \dots, \varphi_n) \iff \tilde{\mathcal{I}} \models \alpha.$$

Analog erhält man auch, dass gilt:

$$\mathcal{I} \models \alpha'(\varphi_1, \dots, \varphi_n) \iff \tilde{\mathcal{I}} \models \alpha'.$$

Laut Voraussetzung sind  $\alpha$  und  $\alpha'$  äquivalente aussagenlogische Formeln. Daher gilt:

$$\tilde{\mathcal{I}} \models \alpha \iff \tilde{\mathcal{I}} \models \alpha'.$$

Somit gilt auch:

$$\mathcal{I} \models \alpha(\varphi_1, \dots, \varphi_n) \iff \mathcal{I} \models \alpha'(\varphi_1, \dots, \varphi_n).$$

Insgesamt erhalten wir, dass  $\alpha(\varphi_1, \dots, \varphi_n)$  und  $\alpha'(\varphi_1, \dots, \varphi_n)$  äquivalente FO[ $\sigma$ ]-Formeln sind.  $\square$

Folie 250

## Quantoren und Negation

Man sieht leicht, dass Folgendes gilt:

**Lemma 3.44.** *Für alle FO[ $\sigma$ ]-Formeln  $\varphi$  und alle Variablen  $x \in \text{VAR}$  gilt:*

$$\neg \exists x \varphi \equiv \forall x \neg \varphi \quad \text{und} \quad \neg \forall x \varphi \equiv \exists x \neg \varphi.$$

*Beweis:* Folgt direkt aus der Definition der Semantik (Details: Übung).  $\square$

Folie 251

## Das Ersetzungslemma

**Lemma 3.45.** *Sei  $\sigma$  eine beliebige Signatur und sei  $\varphi$  eine FO[ $\sigma$ ]-Formel. Ist  $\varphi'$  eine FO[ $\sigma$ ]-Formel, die aus  $\varphi$  entsteht, indem man eine Subformel  $\psi$  von  $\varphi$  durch eine zu  $\psi$  äquivalente FO[ $\sigma$ ]-Formel  $\psi'$  ersetzt, so ist  $\varphi \equiv \varphi'$ .*

*Beweis:* Übung.

**Satz 3.46.** *Jede FO[ $\sigma$ ]-Formel ist äquivalent zu einer FO[ $\sigma$ ]-Formel, in der*

- (a) keiner der Junktoren  $\{\wedge, \rightarrow\}$  vorkommt  
 (d.h., es kommen nur die Junktoren  $\neg, \vee$  und die Quantoren  $\exists, \forall$  vor).
- (b) nur Existenzquantoren und die Junktoren  $\neg, \vee$  vorkommen.
- (c) nur Existenzquantoren und die Junktoren  $\neg, \wedge$  vorkommen.
- (d) nur Allquantoren und die Junktoren  $\neg, \vee$  vorkommen.
- (e) nur Allquantoren und die Junktoren  $\neg, \wedge$  vorkommen.

Daher genügt es, bei Beweisen per Induktion über den Aufbau von Formeln von nun an im Induktionsschritt i.d.R. nur noch die Fälle für  $\exists, \neg, \vee$  zu betrachten.

**Beweis von Satz 3.46:**

Aus Lemma 3.43 folgt, dass „ $\wedge$ “ und „ $\rightarrow$ “ mit Hilfe von „ $\vee$ “ und „ $\neg$ “ ausgedrückt werden können. Somit gilt (a).

Aus Lemma 3.44 folgt, dass „ $\forall$ “ mit Hilfe von „ $\exists$ “ und „ $\neg$ “ ausgedrückt werden. Daher gilt (b).

Da „ $\vee$ “ mit Hilfe von „ $\wedge$ “ und „ $\neg$ “ ausgedrückt werden kann, gilt auch (c).

Außerdem folgt aus Lemma 3.44, dass „ $\exists$ “ mit Hilfe von „ $\forall$ “ und „ $\neg$ “ ausgedrückt werden kann. Aus (b) und (c) folgt daher (d) und (e).  $\square$

### 3.8 Ehrenfeucht-Fraïssé-Spiele

Folie 252

In diesem Abschnitt werden Ehrenfeucht-Fraïssé-Spiele (kurz: EF-Spiele) eingeführt. Diese liefern ein Werkzeug, mit dessen Hilfe man zeigen kann, dass bestimmte Anfragen oder Klassen von Strukturen nicht in Logik erster Stufe definiert werden können.

Der Einfachheit halber betrachten wir hier nur Signaturen, die keine Funktionssymbole und keine Konstantensymbole enthalten. Solche Signaturen werden im Folgenden *relationale Signaturen* genannt.

Außerdem werden wir im Folgenden bei zwei gegebenen Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  immer o.B.d.A. annehmen, dass ihre Universen disjunkt sind, d.h.  $A \cap B = \emptyset$ .

Folie 253

## Das $m$ -Runden EF-Spiel

Sei  $\sigma$  eine relationale Signatur und seien  $\mathcal{A}, \mathcal{B}$  zwei  $\sigma$ -Strukturen.

Für  $k \in \mathbb{N}$  seien  $\bar{a} := a_1, \dots, a_k \in A$  und  $\bar{b} := b_1, \dots, b_k \in B$  Folgen der Länge  $k$  von Elementen aus  $A$  bzw.  $B$ .

Sei  $m \in \mathbb{N}$ .

Das  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  (bzw. auf  $\mathcal{A}$  und  $\mathcal{B}$ , falls  $k = 0$  ist) wird gemäß folgender Spielregeln gespielt:

Folie 254

### Spielregeln des $m$ -Runden EF-Spiels auf $(\mathcal{A}, \bar{a})$ und $(\mathcal{B}, \bar{b})$

- Es gibt 2 Spieler, genannt *Spoiler* (kurz: *Sp*) und *Duplicator* (kurz: *Dupl*).
- Das *Spielbrett* besteht aus  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .
- Eine *Partie* des Spiels besteht aus  $m$  Runden.

In jeder Runde  $i \in \{1, \dots, m\}$  geschieht Folgendes:

1. Zunächst wählt *Spoiler* entweder ein Element in  $A$ , das im Folgenden mit  $a_{k+i}$  bezeichnet wird, oder er wählt ein Element in  $B$ , das im Folgenden mit  $b_{k+i}$  bezeichnet wird.

*Beachte:* Insbes. kann *Spoiler* in jeder Runde neu entscheiden, in welcher der beiden Strukturen er ein Element wählen möchte.

2. Danach antwortet *Duplicator* mit einem Element aus dem Universum der anderen Struktur, d.h. er wählt ein  $b_{k+i} \in B$ , falls *Spoiler* ein  $a_{k+i} \in A$  gewählt hat, bzw. ein Element  $a_{k+i} \in A$ , falls *Spoiler* ein  $b_{k+i} \in B$  gewählt hat.

Nach Runde  $m$  ist die Partie beendet und der Gewinner wird wie folgt ermittelt:

Folie 255

### Gewinnbedingung

*Duplicator* hat gewonnen, falls die beiden folgenden Bedingungen erfüllt sind.

- (1) Für alle  $j, j' \in \{1, \dots, k+m\}$  gilt:  $a_j = a_{j'} \iff b_j = b_{j'}$ .

(2) Die Abbildung  $\pi : \{a_1, \dots, a_{k+m}\} \rightarrow \{b_1, \dots, b_{k+m}\}$  mit

$$\pi(a_j) := b_j, \quad \text{für jedes } j \in \{1, \dots, k+m\}$$

ist ein *partieller Isomorphismus* von  $\mathcal{A}$  nach  $\mathcal{B}$  (siehe Definition 3.47).

Spoiler hat gewonnen, falls mindestens eine der beiden obigen Bedingungen verletzt ist.

**Definition 3.47** (partieller Isomorphismus).

Sei  $\sigma$  eine relationale Signatur, seien  $\mathcal{A}, \mathcal{B}$  zwei  $\sigma$ -Strukturen und sei  $X \subseteq A$ . Eine Abbildung  $\pi : X \rightarrow B$  heißt *partieller Isomorphismus* von  $\mathcal{A}$  nach  $\mathcal{B}$ , falls gilt:

(1)  $\pi$  ist injektiv und

(2) für jedes  $R \in \sigma$ , für  $r := \text{ar}(R)$  und für alle  $(x_1, \dots, x_r) \in X^r$  gilt:

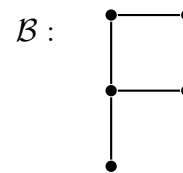
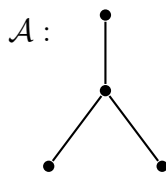
$$(x_1, \dots, x_r) \in R^{\mathcal{A}} \iff (\pi(x_1), \dots, \pi(x_r)) \in R^{\mathcal{B}}.$$

Folie 256

**Beispiel 3.48.** Sei  $\sigma := \{E/2\}$  und sei  $k := 0$ .

In den folgenden Darstellungen von Graphen repräsentiert jede ungerichtete Kante zwischen Knoten  $x$  und  $y$  die beiden gerichteten Kanten  $(x, y)$  und  $(y, x)$ .

(a) Betrachte die folgenden beiden Graphen  $\mathcal{A}, \mathcal{B}$ .



*Spoiler* gewinnt das 2-Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$ , indem er folgendermaßen spielt:

- Runde 1: Wähle denjenigen Knoten  $a_1$  in  $\mathcal{A}$ , der mit allen anderen Knoten durch eine Kante verbunden ist.
- Runde 2: Wähle einen Knoten  $b_2$  in  $\mathcal{B}$ , der nicht zum Knoten  $b_1$  benachbart ist.

(b) Betrachte die beiden folgenden Graphen  $\mathcal{A}, \mathcal{B}$ .



*Duplicator* gewinnt das 2-Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$ , denn in beiden Graphen gibt es zu jedem Knoten sowohl einen Nachbarn, als auch einen Nicht-Nachbarn.

(c) *Spoiler* gewinnt das 3-Runden EF-Spiel auf den Graphen  $\mathcal{A}$  und  $\mathcal{B}$  aus (b), indem er in den ersten 3 Runden 3 verschiedene nicht benachbarte Knoten in  $\mathcal{A}$  wählt.

### Die Ziele von Spoiler und Duplicator

Die Gewinnbedingung im EF-Spiel ist so gewählt, dass die Ziele von Spoiler und Duplicator anschaulich folgendermaßen beschrieben werden können:

- *Spoilers Ziel* ist es, zu zeigen, dass die beiden Strukturen  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  verschieden sind.
- *Duplicators Ziel* ist es, einen etwaigen Unterschied zwischen den beiden Strukturen zu vertuschen.

### Gewinnstrategien

Eine *Strategie* für einen der beiden Spieler im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  ist eine Vorschrift, die ihm sagt, welchen Zug er als Nächstes machen soll. Formal:

- Eine *Strategie für Spoiler* ist eine Abbildung

$$f_{Sp} : \bigcup_{i=0}^{m-1} (A \times B)^i \longrightarrow A \cup B.$$

Sind  $a_{k+1}, \dots, a_{k+i} \in A$  und  $b_{k+1}, \dots, b_{k+i} \in B$  die in den ersten  $i$  Runden gewählten Elemente, so gibt

$$f_{Sp}(a_{k+1}, b_{k+1}, \dots, a_{k+i}, b_{k+i})$$

an, welches Element Spoiler in der  $(i+1)$ -ten Runde wählen soll.

Folie 260

- Eine *Strategie für Duplicator* ist eine Abbildung

$$f_{Dupl} : \bigcup_{i=0}^{m-1} (A \times B)^i \times (A \cup B) \longrightarrow B \cup A,$$

so dass für alle  $i \in \{0, \dots, m-1\}$ , alle  $a_{k+1}, \dots, a_{k+i} \in A$ , alle  $b_{k+1}, \dots, b_{k+i} \in B$  und alle  $c_{k+i+1} \in A \cup B$  gilt:

$$c_{k+i+1} \in A \iff f_{Dupl}(a_{k+1}, b_{k+1}, \dots, a_{k+i}, b_{k+i}, c_{k+i+1}) \in B.$$

Sind  $a_{k+1}, \dots, a_{k+i} \in A$  und  $b_{k+1}, \dots, b_{k+i} \in B$  die in den ersten  $i$  Runden und ist  $c_{k+i+1} \in A \cup B$  das von Spoiler in Runde  $i+1$  gewählte Element, so gibt

$$f_{Dupl}(a_{k+1}, b_{k+1}, \dots, a_{k+i}, b_{k+i}, c_{k+i+1})$$

an, welches Element Duplicator in der  $(i+1)$ -ten Runde wählen soll.

- Eine *Gewinnstrategie* ist eine Strategie für einen der beiden Spieler, mit der er jede Partie des  $m$ -Runden EF-Spiels auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  gewinnt.

Folie 261

## Der Satz von Ehrenfeucht

Sei  $\sigma$  eine relationale Signatur, seien  $\mathcal{A}, \mathcal{B}$  zwei  $\sigma$ -Strukturen, sei  $m \in \mathbb{N}$ , sei  $k \in \mathbb{N}$ , sei  $\bar{a} = a_1, \dots, a_k \in A$  und  $\bar{b} = b_1, \dots, b_k \in B$ .

Der Satz von Ehrenfeucht besagt, dass die beiden folgenden Aussagen äquivalent sind:

- (1) Duplicator hat eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .
- (2) Für jede FO[ $\sigma$ ]-Formel  $\varphi(x_1, \dots, x_k)$  der Quantorentiefe  $\leq m$  gilt:

$$\mathcal{A} \models \varphi[a_1, \dots, a_k] \iff \mathcal{B} \models \varphi[b_1, \dots, b_k].$$

Anschaulich bedeutet dies, dass  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  aus Perspektive von FO[ $\sigma$ ]-Formeln der Quantorentiefe  $\leq m$  „gleich“ aussehen, d.h. dass  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  von solchen Formeln nicht unterschieden werden können.

Die Quantorentiefe einer Formel  $\varphi$  ist dabei die maximale Anzahl von ineinander geschachtelten Quantoren, die in  $\varphi$  vorkommen:

Folie 262

**Definition 3.49.** Die *Quantorentiefe* (bzw. der *Quantorenrang*, engl.: *quantifier rank*)  $\text{qr}(\varphi)$  einer FO[ $\sigma$ ]-Formel  $\varphi$  ist rekursiv wie folgt definiert:

- Ist  $\varphi$  *atomar*, so ist  $\text{qr}(\varphi) := 0$ .
- Ist  $\varphi$  von der Form  $\neg\psi$ , so ist  $\text{qr}(\varphi) := \text{qr}(\psi)$ .
- Ist  $\varphi$  von der Form  $(\psi_1 * \psi_2)$  mit  $*$   $\in \{\wedge, \vee, \rightarrow\}$ , so ist  $\text{qr}(\varphi) := \max\{\text{qr}(\psi_1), \text{qr}(\psi_2)\}$ .
- Ist  $\varphi$  von der Form  $\exists x \psi$  oder  $\forall x \psi$ , so ist  $\text{qr}(\varphi) := \text{qr}(\psi) + 1$ .

*Beispiele:*

- $\text{qr}(\exists x \forall y (x=y \vee E(x, y))) = 2$ .
- $\text{qr}(\exists x (E(x, x) \vee \forall y \neg E(x, y))) = 2$ .
- $\text{qr}((\exists x E(x, x) \vee \forall y \neg E(x, y))) = 1$ .

**Bemerkung 3.50.** Gemäß Satz 3.46 ist jede FO[ $\sigma$ ]-Formel  $\varphi$  äquivalent zu einer FO[ $\sigma$ ]-Formel  $\varphi'$ , in der nur Existenzquantoren und die Junktoren  $\neg, \vee$  vorkommen (d.h.: in  $\varphi'$  kommt keins der Symbole  $\forall, \wedge, \rightarrow$  vor).

Man sieht leicht, dass  $\varphi'$  sogar so gewählt werden kann, dass gilt:  
 $\text{qr}(\varphi') = \text{qr}(\varphi)$  und  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

Folie 263

Wir beweisen hier nur die Richtung „(1)  $\implies$  (2)“ des Satzes von Ehrenfeucht, deren Kontraposition in folgendem Satz formuliert wird.

**Satz 3.51** (Satz von Ehrenfeucht, einfache Version).

Sei  $\sigma$  eine relationale Signatur und seien  $\mathcal{A}, \mathcal{B}$  zwei  $\sigma$ -Strukturen, sei  $m \in \mathbb{N}$ , sei  $k \in \mathbb{N}$ , sei  $\bar{a} = a_1, \dots, a_k \in A$  und sei  $\bar{b} = b_1, \dots, b_k \in B$ . Falls es eine FO[ $\sigma$ ]-Formel  $\varphi(x_1, \dots, x_k)$  mit  $\text{frei}(\varphi) \subseteq \{x_1, \dots, x_k\}$  und  $\text{qr}(\varphi) \leq m$  gibt, so dass

$$\mathcal{A} \models \varphi[a_1, \dots, a_k] \quad \text{und} \quad \mathcal{B} \not\models \varphi[b_1, \dots, b_k],$$

so hat Spoiler eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

Folie 264

### Beweisidee

Zunächst illustrieren wir die Beweisidee an einem Beispiel. Betrachte dazu die Formel

$$\varphi := \exists x_1 \forall x_2 (x_1 = x_2 \vee E(x_1, x_2))$$

und die beiden Graphen  $\mathcal{A}, \mathcal{B}$  aus Beispiel 3.48(a).



Es gilt:  $\mathcal{A} \models \varphi$  und  $\mathcal{B} \not\models \varphi$ , d.h.  $\mathcal{B} \models \neg\varphi$ .

Klar:

$$\neg\varphi \equiv \forall x_1 \exists x_2 (\neg x_1 = x_2 \wedge \neg E(x_1, x_2)).$$

Also gilt:



$$\mathcal{A} \models \exists x_1 \forall x_2 (x_1 = x_2 \vee E(x_1, x_2)) \quad (3.2)$$

und

$$\mathcal{B} \models \forall x_1 \exists x_2 (\neg x_1 = x_2 \wedge \neg E(x_1, x_2)) \quad (3.3)$$

Eine Gewinnstrategie für Spoiler im 2-Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$  lässt sich daran direkt ablesen — Spoiler gewinnt, indem er wie folgt „die Formel  $\varphi$  ausspielt“:

Wegen (3.2) kann Spoiler in Runde 1 ein  $a_1 \in A$  wählen, so dass gilt:

$$\mathcal{A} \models \left( \forall x_2 (x_1 = x_2 \vee E(x_1, x_2)) \right) [a_1] \quad (3.4)$$

Dieses  $a_1$  ist gerade der Knoten „in der Mitte“ des Graphen  $\mathcal{A}$ , d.h. der Knoten, der Kanten zu allen anderen Knoten von  $\mathcal{A}$  besitzt.

Wegen (3.3) gilt dann für jedes Element  $b_1 \in B$ , mit dem Duplicator in Runde 1 antworten könnte, dass

$$\mathcal{B} \models \left( \exists x_2 (\neg x_1 = x_2 \wedge \neg E(x_1, x_2)) \right) [b_1] \quad (3.5)$$

In Runde 2 kann Spoiler daher ein Element  $b_2 \in B$  auswählen, für das gilt:

$$\mathcal{B} \models \left( \neg x_1 = x_2 \wedge \neg E(x_1, x_2) \right) [b_1, b_2] \quad (3.6)$$

Wegen (3.4) gilt für jedes Element  $a_2 \in A$ , mit dem Duplicator in Runde 2 antworten könnte, dass

$$\mathcal{A} \models \left( x_1 = x_2 \vee E(x_1, x_2) \right) [a_1, a_2] \quad (3.7)$$

Am Ende der Partie wissen wir gemäß (3.7) und (3.6) also, dass Folgendes gilt:

$$\left( a_1 = a_2 \text{ oder } (a_1, a_2) \in E^{\mathcal{A}} \right) \text{ und } \left( b_1 \neq b_2 \text{ und } (b_1, b_2) \notin E^{\mathcal{B}} \right)$$

Falls  $a_1 = a_2$  ist, so ist Teil (1) der Gewinnbedingung für Duplicator verletzt; falls  $(a_1, a_2) \in E^{\mathcal{A}}$  ist, so ist Teil (2) der Gewinnbedingung für Duplicator verletzt. Also gewinnt Spoiler jede Partie des 2-Runden EF-Spiels auf  $\mathcal{A}$  und  $\mathcal{B}$ .

Somit hat Spoiler eine Gewinnstrategie im 2-Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$ .

**Beweis von Satz 3.51:**

Wir führen den Beweis per Induktion über den Aufbau von Formeln. Es seien eine relationale Signatur  $\sigma$  und zwei  $\sigma$ -Strukturen  $\mathcal{A}$  und  $\mathcal{B}$  gegeben. Die Aussage  $\mathbb{A}(\varphi)$ , die wir für alle FO[ $\sigma$ ]-Formeln  $\varphi$  beweisen wollen, besagt Folgendes:

Für alle  $m, k \in \mathbb{N}$ , alle  $\bar{a} = a_1, \dots, a_k \in A$  und alle  $\bar{b} = b_1, \dots, b_k \in B$  gilt:

Falls  $\text{qr}(\varphi) \leq m$  und  $|\text{frei}(\varphi)| \leq k$  und

$$\mathcal{A} \models \varphi[a_1, \dots, a_k] \iff \mathcal{B} \not\models \varphi[b_1, \dots, b_k],$$

so hat Spoiler eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

Um  $\mathbb{A}(\varphi)$  für eine gegebene Formel  $\varphi$  zu beweisen, seien im Folgenden  $m, k \in \mathbb{N}$ ,  $\bar{a} = a_1, \dots, a_k \in A$  und  $\bar{b} = b_1, \dots, b_k \in B$  beliebig gewählt. Es genügt, den Fall zu betrachten, in dem gilt:

$$(*) : \quad m \geq \text{qr}(\varphi), \quad k \geq |\text{frei}(\varphi)| \quad \text{und} \quad \mathcal{A} \models \varphi[\bar{a}] \iff \mathcal{B} \not\models \varphi[\bar{b}],$$

denn andernfalls muss gemäß der Formulierung von  $\mathbb{A}(\varphi)$  nichts gezeigt werden.

Ziel ist, zu zeigen, dass Spoiler eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  hat.

*Induktionsanfang:* Sei  $\varphi$  atomar. Da  $\sigma$  eine *relationale* Signatur ist, sind Variablen die einzigen  $\sigma$ -Terme, d.h.:  $\text{T}_\sigma = \text{VAR}$ . Somit ist jede atomare  $\sigma$ -Formel von einer der beiden im Folgenden betrachteten Formen.

- $\varphi$  ist von der Form  $x_{i_1} = x_{i_2}$ , mit  $i_1, i_2 \in \{1, \dots, k\}$

Wegen (\*) gilt dann insbesondere:

$$a_{i_1} = a_{i_2} \iff b_{i_1} \neq b_{i_2}.$$

Somit ist Duplicators Gewinnbedingung (1) verletzt, und Spoiler gewinnt jede Partie des  $m$ -Runden EF-Spiels auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

- $\varphi$  ist von der Form  $R(x_{i_1}, \dots, x_{i_r})$ , wobei  $R \in \sigma$ ,  $r := \text{ar}(R)$  und  $i_1, \dots, i_r \in \{1, \dots, k\}$ .

Wegen (\*) gilt dann insbesondere:

$$(a_{i_1}, \dots, a_{i_r}) \in R^A \iff (b_{i_1}, \dots, b_{i_r}) \notin R^B.$$

Somit ist Duplicators Gewinnbedingung (2) verletzt, und Spoiler gewinnt jede Partie des  $m$ -Runden EF-Spiels auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

*Induktionsschritt:* Sei  $\varphi$  eine beliebige nicht-atomare FO[ $\sigma$ ]-Formel. Gemäß Bemerkung 3.50 genügt es, im Folgenden die Fälle zu betrachten, in denen  $\varphi$  von einer der folgenden Formen ist:  $\exists y \psi$ ,  $\neg\psi$ ,  $(\psi_1 \vee \psi_2)$ .

- **Fall 1:**  $\varphi$  ist von der Form  $\exists y \psi$ .

Gemäß Induktionsannahme gilt  $\mathbb{A}(\psi)$ .

Unser Ziel ist, zu zeigen, dass Spoiler eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  hat.

Gemäß (\*) gilt:  $m \geq \text{qr}(\varphi)$ ,  $k \geq |\text{frei}(\varphi)|$ ,  $\mathcal{A} \models \varphi[\bar{a}] \iff \mathcal{B} \not\models \varphi[\bar{b}]$ .

*Fall 1.1:*  $\mathcal{A} \models \varphi[\bar{a}]$  und  $\mathcal{B} \not\models \varphi[\bar{b}]$ .

Da  $\varphi$  von der Form  $\exists x \psi$  ist, gilt also:

$$\mathcal{A} \models (\exists x \psi) [\bar{a}] \quad \text{und} \quad \mathcal{B} \models (\forall x \neg\psi) [\bar{b}]$$

Somit gibt es ein  $a_{k+1} \in A$ , so dass gilt:  $\mathcal{A} \models \psi[\bar{a}, a_{k+1}]$ .

Und für jedes  $b_{k+1} \in B$  gilt:  $\mathcal{B} \models \neg\psi[\bar{b}, b_{k+1}]$ .

Spoiler kann daher in Runde 1 ein  $a_{k+1} \in A$  mit  $\mathcal{A} \models \psi[\bar{a}, a_{k+1}]$  wählen. Für jedes  $b_{k+1} \in B$ , mit dem Duplicator in Runde 1 antworten kann, gilt:  $\mathcal{B} \models \neg\psi[\bar{b}, b_{k+1}]$ .

Es gilt:

- $\text{qr}(\psi) = \text{qr}(\varphi) - 1 \leq m-1 =: m'$ ,
- $|\text{frei}(\psi)| \leq |\text{frei}(\varphi)| + 1 \leq k+1 =: k'$ , und
- für  $\bar{a}' := a_1, \dots, a_k, a_{k+1}$  und  $\bar{b}' := b_1, \dots, b_k, b_{k+1}$  gilt:

$$\mathcal{A} \models \psi[\bar{a}'] \quad \text{und} \quad \mathcal{B} \not\models \psi[\bar{b}'].$$

Da  $\mathbb{A}(\psi)$  gemäß Induktionsannahme gilt, hat Spoiler daher eine Gewinnstrategie im  $m'$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a}')$  und  $(\mathcal{B}, \bar{b}')$ .

Für das  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  erhält Spoiler daher eine Gewinnstrategie, indem er in Runde 1 ein  $a_{k+1} \in A$  wählt, so dass gilt:  $\mathcal{A} \models \psi[\bar{a}, a_{k+1}]$ .

Für jedes  $b_{k+1} \in B$ , mit dem Duplicator in Runde 1 antworten kann, spielt Spoiler die restlichen  $m' = m-1$  Runden dann gemäß seiner Gewinnstrategie im  $(m-1)$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a}, a_{k+1})$  und  $(\mathcal{B}, \bar{b}, b_{k+1})$ .

*Fall 1.2:*  $\mathcal{B} \models \varphi[\bar{b}]$  und  $\mathcal{A} \not\models \varphi[\bar{a}]$ .

Da  $\varphi$  von der Form  $\exists x \psi$  ist, gilt also:

$$\mathcal{B} \models (\exists x \psi) [\bar{b}] \quad \text{und} \quad \mathcal{A} \models (\forall x \neg \psi) [\bar{a}]$$

Somit gibt es ein  $b_{k+1} \in B$ , so dass gilt:  $\mathcal{B} \models \psi[\bar{b}, b_{k+1}]$ .

Und für jedes  $a_{k+1} \in A$  gilt:  $\mathcal{A} \models \neg \psi[\bar{a}, a_{k+1}]$ .

Spoiler kann daher in Runde 1 ein  $b_{k+1} \in B$  mit  $\mathcal{B} \models \psi[\bar{b}, b_{k+1}]$  wählen. Für jedes  $a_{k+1} \in A$ , mit dem Duplicator in Runde 1 antworten kann, gilt:  $\mathcal{A} \models \neg \psi[\bar{a}, a_{k+1}]$ .

Genau wie in Fall 1.1 hat Spoiler gemäß Induktionsannahme eine Gewinnstrategie im  $(m-1)$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a}, a_{k+1})$  und  $(\mathcal{B}, \bar{b}, b_{k+1})$ .

Insgesamt liefert dies eine Gewinnstrategie für Spoiler im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

- **Fall 2:**  $\varphi$  ist von der Form  $\neg \psi$ .

Gemäß Induktionsannahme gilt  $\mathbb{A}(\psi)$ .

Gemäß (\*) gilt:  $m \geq \text{qr}(\varphi)$ ,  $k \geq |\text{frei}(\varphi)|$ ,  $\mathcal{A} \models \varphi[\bar{a}] \iff \mathcal{B} \not\models \varphi[\bar{b}]$ .

Da  $\varphi$  von der Form  $\neg \psi$  ist, gilt:

$$\text{qr}(\psi) = \text{qr}(\varphi), \quad \text{frei}(\psi) = \text{frei}(\varphi), \quad \mathcal{A} \not\models \psi[\bar{a}] \iff \mathcal{B} \models \psi[\bar{b}].$$

Da  $\mathbb{A}(\psi)$  gemäß Induktionsannahme gilt, hat Spoiler also eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

- **Fall 3:**  $\varphi$  ist von der Form  $(\psi_1 \vee \psi_2)$ .

Gemäß Induktionsannahme gilt  $\mathbb{A}(\psi_1)$  und  $\mathbb{A}(\psi_2)$ .

Gemäß (\*) gilt:  $m \geq \text{qr}(\varphi)$ ,  $k \geq |\text{frei}(\varphi)|$ ,  $\mathcal{A} \models \varphi[\bar{a}] \iff \mathcal{B} \not\models \varphi[\bar{b}]$ .

Da  $\varphi$  von der Form  $(\psi_1 \vee \psi_2)$  ist, sieht man leicht, dass es ein  $i \in \{1, 2\}$  geben muss, so dass gilt:

$$\mathcal{A} \models \psi_i[\bar{a}] \quad \iff \quad \mathcal{B} \not\models \psi_i[\bar{b}]$$

Außerdem gilt:  $\text{qr}(\psi_i) \leq \text{qr}(\varphi) \leq m$ , und  $|\text{frei}(\psi_i)| \leq |\text{frei}(\varphi)| \leq k$ .

Da  $\mathbb{A}(\psi_i)$  gemäß Induktionsannahme gilt, hat Spoiler also eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

Dies beendet den Beweis von Satz 3.51. □

Folie 266

### Folgerung aus dem Satz von Ehrenfeucht

**Notation 3.52.** Eine Klasse  $\mathfrak{C}$  von  $\sigma$ -Strukturen heißt *FO-definierbar*, falls es einen FO[ $\sigma$ ]-Satz  $\varphi$  gibt, der  $\mathfrak{C}$  definiert.

*Zur Erinnerung:*

Für einen FO[ $\sigma$ ]-Satz  $\varphi$  und eine Klasse  $\mathfrak{C}$  von  $\sigma$ -Strukturen sagen wir „ $\varphi$  definiert  $\mathfrak{C}$ “, falls für jede  $\sigma$ -Struktur  $\mathcal{A}$  gilt:  $\mathcal{A} \in \mathfrak{C} \iff \mathcal{A} \models \varphi$ .

Um für eine gegebene Klasse  $\mathfrak{C}$  von  $\sigma$ -Strukturen zu zeigen, dass sie nicht FO-definierbar ist, können wir das folgende Korollar nutzen, das wir als eine einfache Folgerung aus Satz 3.51 erhalten.

#### Korollar 3.53.

*Sei  $\sigma$  eine relationale Signatur und sei  $\mathfrak{C}$  eine Klasse von  $\sigma$ -Strukturen. Falls es für jedes  $m \geq 1$  zwei  $\sigma$ -Strukturen  $\mathcal{A}_m$  und  $\mathcal{B}_m$  gibt, so dass gilt:*

1.  $\mathcal{A}_m \in \mathfrak{C}$  und
2.  $\mathcal{B}_m \notin \mathfrak{C}$  und
3. *Duplicator hat eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$ ,*

*dann ist  $\mathfrak{C}$  nicht FO-definierbar.*

*Beweis.*

Für jedes  $m \geq 1$  seien  $\mathcal{A}_m$  und  $\mathcal{B}_m$  zwei  $\sigma$ -Strukturen, so dass 1.–3. gilt. Wir führen einen Beweis durch Widerspruch und nehmen an, dass  $\mathfrak{C}$  doch FO-definierbar ist. D.h. es gibt einen FO[ $\sigma$ ]-Satz  $\varphi$ , der  $\mathfrak{C}$  definiert. Somit gilt für jede  $\sigma$ -Struktur  $\mathcal{C}$ :

$$\mathcal{C} \models \varphi \iff \mathcal{C} \in \mathfrak{C}. \quad (3.8)$$

Betrachte die Strukturen  $\mathcal{A}_m$  und  $\mathcal{B}_m$  für ein  $m$  mit  $m \geq \text{qr}(\varphi)$ . Laut Voraussetzung wissen wir, dass 1.–3. gilt.

Wegen  $\mathcal{A}_m \in \mathfrak{C}$  und  $\mathcal{B}_m \notin \mathfrak{C}$  gilt gemäß (3.8), dass

$$\mathcal{A}_m \models \varphi \quad \text{und} \quad \mathcal{B}_m \not\models \varphi.$$

Gemäß Satz 3.51 (Satz von Ehrenfeucht, einfache Version) hat Spoiler also eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$ . Dies ist ein Widerspruch zu 3., da gemäß 3. Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$  hat.  $\square$

Folie 267

## Lineare Ordnungen gerader Kardinalität

Wir werden nun Korollar 3.53 anwenden, um folgenden Satz zu zeigen.

**Satz 3.54.** *Die Klasse  $EVEN_{\leq}$ , die aus allen linearen Ordnungen  $\mathcal{A} = (A, \leq^{\mathcal{A}})$  gerader Kardinalität besteht (d.h.,  $A$  ist endlich und  $|A|$  ist durch 2 teilbar), ist nicht FO-definierbar.*

Um diesen Satz zu beweisen, genügt es gemäß Korollar 3.53, für jede Rundenzahl  $m \geq 1$  eine lineare Ordnung  $\mathcal{A}_m$  gerader Kardinalität und eine lineare Ordnung  $\mathcal{B}_m$  ungerader Kardinalität anzugeben, für die wir zeigen können, dass Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$  hat.

Folie 268

Als Vorbereitung dazu betrachten wir zunächst ein Beispiel.

### Beispiel 3.55.

Betrachte die linearen Ordnungen  $\mathcal{A} = (A, \leq^{\mathcal{A}})$  und  $\mathcal{B} = (B, \leq^{\mathcal{B}})$  mit  $A = \{1, \dots, 8\}$  und  $B = \{1, \dots, 9\}$ , wobei  $\leq^{\mathcal{A}}$  und  $\leq^{\mathcal{B}}$  die natürlichen linearen Ordnungen auf  $A$  und  $B$  sind.

Seien außerdem  $k := 2$  und  $\bar{a} := a_1, a_2$  und  $\bar{b} := b_1, b_2$  mit  $a_1 = b_1 = 1$  und  $a_2 = 8$  und  $b_2 = 9$  vorgegeben.

*Frage:* Was ist die größte Zahl  $m$ , so dass Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$  hat?

*Antwort:* Duplicator hat eine Gewinnstrategie im 2-Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ ; Spoiler hat eine Gewinnstrategie im 3-Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

Folie 269

Die Gewinnstrategie für Duplicator lässt sich zu folgendem Resultat verallgemeinern.

**Lemma 3.56.** Seien  $\mathcal{A}$  und  $\mathcal{B}$  endliche<sup>3</sup> lineare Ordnungen, sei  $k := 2$ , und sei  $\bar{a} := a_1, a_2$  und  $\bar{b} := b_1, b_2$ , wobei  $a_1, b_1$  die kleinsten und  $a_2, b_2$  die größten Elemente in  $A$  und  $B$  bezüglich  $\leq^{\mathcal{A}}$  und  $\leq^{\mathcal{B}}$  sind.

Für jedes  $m \geq 1$  gilt: Falls  $|A|, |B| > 2^m$  oder  $|A| = |B|$ , so hat Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ .

*Beweis.*

Falls  $|A| = |B|$ , so sind  $\mathcal{A}$  und  $\mathcal{B}$  isomorph (beachte dazu: laut Voraussetzung sind  $A$  und  $B$  endlich). Sei  $\pi : \mathcal{A} \cong \mathcal{B}$  ein Isomorphismus von  $\mathcal{A}$  nach  $\mathcal{B}$ . Duplicator gewinnt das  $m$ -Runden EF-Spiel auf  $(\mathcal{A}, \bar{a})$  und  $(\mathcal{B}, \bar{b})$ , indem er in jeder Runde  $i \in \{1, \dots, m\}$  einfach Spoilers Zug „kopiert“, d.h. er wählt  $\pi(a_{k+i})$  (bzw.  $\pi^{-1}(b_{k+i})$ ), wenn Spoiler in Runde  $i$  ein Element  $a_{k+i} \in A$  (bzw.  $b_{k+i} \in B$ ) wählt.

Im Folgenden betrachten wir den Fall, dass  $|A| > 2^m$  und  $|B| > 2^m$ .

Für jedes  $C \in \{\mathcal{A}, \mathcal{B}\}$  betrachte die Distanzfunktion  $Dist : C \times C \rightarrow \mathbb{N}$  mit

$$Dist(c, c') := |\{d \in C : c <^C d \leq^C c' \text{ oder } c' <^C d \leq^C c\}|$$

für alle  $c, c' \in C$ .

Folie 270

Wir zeigen nun, dass Duplicator so spielen kann, dass für jedes  $i \in \{0, 1, \dots, m\}$  die folgende Invariante  $(*)_i$  erfüllt ist:

$(*)_i$ : Sind  $a_{2+1}, \dots, a_{2+i}$  und  $b_{2+1}, \dots, b_{2+i}$  die in den Runden  $1, \dots, i$  gewählten Elemente in  $A$  und  $B$ , so gilt für alle  $j, j' \in \{1, \dots, 2+i\}$ :

1.  $a_j \leq^{\mathcal{A}} a_{j'} \iff b_j \leq^{\mathcal{B}} b_{j'}$  und
2.  $Dist(a_j, a_{j'}) = Dist(b_j, b_{j'})$  oder  $Dist(a_j, a_{j'}) \geq 2^{m-i}$  oder  $Dist(b_j, b_{j'}) \geq 2^{m-i}$ .

Der Beweis folgt per Induktion nach  $i$ .

*Induktionsanfang:*  $i=0$

Die Bedingung  $(*)_0$  ist erfüllt, denn laut Voraussetzung gilt:

$$Dist(a_1, a_2) = |A| - 1 \geq 2^m \quad \text{und} \quad Dist(b_1, b_2) = |B| - 1 \geq 2^m.$$

*Induktionsschritt:*  $i \rightarrow i+1$

Gemäß Induktionsannahme sind bereits  $i$  Runden gespielt und die Bedingung  $(*)_i$  ist nach der  $i$ -ten Runde erfüllt.

<sup>3</sup>d.h., die Universen von  $\mathcal{A}$  und  $\mathcal{B}$  sind endlich

*Fall 1:* Spoiler wählt in der  $(i+1)$ -ten Runde ein Element  $a_{2+i+1}$  in  $A$ . Falls  $a_{2+i+1} = a_j$  für ein  $j \in \{1, \dots, 2+i\}$ , so antwortet Duplicator mit  $b_{2+i+1} := b_j$  und bewirkt damit, dass die Bedingung  $(*)_{i+1}$  erfüllt ist. Ansonsten gibt es Indizes  $j, j' \in \{1, \dots, 2+i\}$ , so dass gilt:

- $a_j <^A a_{2+i+1} <^A a_{j'}$  und
- für alle  $j'' \in \{1, \dots, 2+i\}$  gilt:  $a_{j''} \leq^A a_j$  oder  $a_{j''} \leq^A a_{j'}$ .

Da  $(*)_i$  gemäß Induktionsannahme erfüllt ist, gilt:

- (1.)  $Dist(a_j, a_{j'}) = Dist(b_j, b_{j'})$  oder
- (2.)  $Dist(a_j, a_{j'}), Dist(b_j, b_{j'}) \geq 2^{m-i}$ .

Im Fall (1.) gibt es ein Element  $b_{2+i+1}$  in  $B$ , so dass  $b_j <^B b_{2+i+1} <^B b_{j'}$  und  $Dist(b_j, b_{2+i+1}) = Dist(a_j, a_{2+i+1})$  und  $Dist(b_{2+i+1}, b_{j'}) = Dist(a_{2+i+1}, a_{j'})$ . Man kann sich leicht davon überzeugen, dass die Bedingung  $(*)_{i+1}$  erfüllt ist, wenn Duplicator in der  $(i+1)$ -ten Runde dieses  $b_{2+i+1}$  wählt.

Im Fall (2.) muss es mindestens ein Element  $c \in B$  geben, so dass  $b_j <^B c <^B b_{j'}$  und  $Dist(b_j, c) \geq \frac{2^{m-i}}{2} = 2^{m-(i+1)}$  und  $Dist(c, b_{j'}) \geq \frac{2^{m-i}}{2} = 2^{m-(i+1)}$ .

- Falls  $Dist(a_j, a_{2+i+1}) \geq 2^{m-(i+1)}$  und  $Dist(a_{2+i+1}, a_{j'}) \geq 2^{m-(i+1)}$ , so wählt Duplicator in der  $(i+1)$ -ten Runde  $b_{2+i+1} := c$ .
- Falls  $Dist(a_j, a_{2+i+1}) < 2^{m-(i+1)}$ , so wählt Duplicator das  $b_{2+i+1} >^B b_j$  mit  $Dist(b_j, b_{2+i+1}) = Dist(a_j, a_{2+i+1})$ .
- Falls  $Dist(a_{2+i+1}, a_{j'}) < 2^{m-(i+1)}$ , so wählt Duplicator das  $b_{2+i+1} <^B b_{j'}$  mit  $Dist(b_{2+i+1}, b_{j'}) = Dist(a_{2+i+1}, a_{j'})$ .

Man kann leicht nachprüfen, dass in jedem der 3 Fälle die Bedingung  $(*)_{i+1}$  erfüllt ist.

*Fall 2:* Spoiler wählt in der  $(i+1)$ -ten Runde ein Element  $b_{2+i+1}$  in  $B$ . Duplicators Antwort  $a_{2+i+1}$  in  $A$  wird analog zu Fall 1 ermittelt.

Damit sind wir fertig mit dem Induktionsschritt.

Wir haben also bewiesen, dass Duplicator, so spielen kann, dass für jedes  $i \in \{0, 1, \dots, m\}$  die Bedingung  $(*)_i$  erfüllt ist.

Insbesondere ist nach Runde  $m$  die Bedingung  $(*)_m$  erfüllt und Duplicator hat daher die Partie gewonnen. □



Satz 3.54 folgt nun direkt aus Korollar 3.53 und Lemma 3.56.

**Beweis von Satz 3.54.**

Um nachzuweisen, dass die Klasse  $EVEN_{\leq}$  nicht FO-definierbar ist, genügt es laut Korollar 3.53, für jede Zahl  $m \geq 1$  eine endliche lineare Ordnung  $\mathcal{A}_m$  gerader Kardinalität und eine endliche lineare Ordnung  $\mathcal{B}_m$  ungerader Kardinalität zu finden, so dass Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$  besitzt.

Wir wählen für  $\mathcal{A}_m$  die natürliche lineare Ordnung mit Universum  $A_m := \{1, \dots, 2^m + 2\}$ , und für  $\mathcal{B}_m$  die natürliche lineare Ordnung mit Universum  $B_m := \{1, \dots, 2^m + 1\}$ .

Gemäß Lemma 3.56 hat Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $(\mathcal{A}_m, \bar{a})$  und  $(\mathcal{B}_m, \bar{b})$ , wobei  $\bar{a} = a_1, a_2$  und  $\bar{b} = b_1, b_2$  jeweils aus dem kleinsten und dem größten Element der beiden linearen Ordnungen bestehen.

Offensichtlicherweise ist diese Gewinnstrategie auch eine Gewinnstrategie für Duplicator im  $m$ -Runden EF-Spiel auf  $\mathcal{A}_m$  und  $\mathcal{B}_m$ .  $\square$

**Bemerkung 3.57.**

Der obige Beweis zeigt nicht nur, dass die Klasse  $EVEN_{\leq}$  nicht FO-definierbar ist, sondern sogar die folgende stärkere Aussage:

*Für jedes  $n \in \mathbb{N}$  gilt: Es gibt keinen FO[ $\{\leq\}$ ]-Satz  $\psi$ , so dass für jede **endliche lineare Ordnung**  $\mathcal{B}$  mit  $|B| \geq n$  gilt:*

$$\mathcal{B} \models \psi \iff |B| \text{ ist gerade.}$$

*Beweis.* Durch Widerspruch.

Sei  $n \in \mathbb{N}$  beliebig gewählt. Angenommen, es gibt einen FO[ $\{\leq\}$ ]-Satz  $\psi$ , so dass für jede endliche lineare Ordnung  $\mathcal{B}$  mit  $|B| \geq n$  gilt:

$$\mathcal{B} \models \psi \iff |B| \text{ ist gerade.}$$

Dann sei  $m := \text{qr}(\psi)$ . Wähle ein  $\ell \in \mathbb{N}$  mit  $\ell \geq m$  und  $2^\ell \geq n$ . Sei  $\mathcal{A}$  eine lineare Ordnung auf genau  $2^\ell + 1$  Elementen und sei  $\mathcal{B}$  eine lineare Ordnung auf genau  $2^\ell + 2$  Elementen.

Da  $|A| \geq n$  und gerade ist, gilt:  $\mathcal{A} \models \psi$ .

Da  $|B| \geq n$  und ungerade ist, gilt:  $\mathcal{B} \not\models \psi$ .

Gemäß Satz 3.51 hat Spoiler eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$ . Aber aus Lemma 3.56 folgt, dass Duplicator eine Gewinnstrategie im  $m$ -Runden EF-Spiel auf  $\mathcal{A}$  und  $\mathcal{B}$  hat. Widerspruch!  $\square$

## Graph-Zusammenhang und Erreichbarkeit sind nicht FO-definierbar

Wir können die Aussage von Bemerkung 3.57 nutzen, um Folgendes zu zeigen.

**Satz 3.58.** Sei  $\sigma := \{E/2\}$ .

(a) „Graph-Zusammenhang ist nicht FO-definierbar.“

*D.h.:* Es gibt keinen FO[ $\sigma$ ]-Satz  $\varphi_{Conn}$ , so dass für jeden endlichen ungerichteten Graphen  $\mathcal{G} = (V^{\mathcal{G}}, E^{\mathcal{G}})$  und die zugehörige<sup>4</sup>  $\sigma$ -Struktur  $\mathcal{A} = (A, E^{\mathcal{A}})$  gilt:  $\mathcal{A} \models \varphi_{Conn} \iff \mathcal{G}$  ist zusammenhängend.

(b) „Erreichbarkeit ist nicht FO-definierbar.“

*D.h.:* Es gibt keine FO[ $\sigma$ ]-Formel  $\varphi_{Reach}(x, y)$ , so dass für alle endlichen gerichteten Graphen  $\mathcal{A} = (A, E^{\mathcal{A}})$  und alle Knoten  $a, b \in A$  gilt:  $\mathcal{A} \models \varphi_{Reach}[a, b] \iff$  es gibt in  $\mathcal{A}$  einen Weg von Knoten  $a$  zu Knoten  $b$ .

*Beweis.*

(a): Wir führen einen Beweis durch Widerspruch und nutzen Bemerkung 3.57.

Angenommen,  $\varphi_{Conn}$  ist ein FO[ $\sigma$ ]-Satz, so dass für jeden endlichen ungerichteten Graphen  $\mathcal{G}$  und die zugehörige  $\sigma$ -Struktur  $\mathcal{A}$  gilt:

$$\mathcal{A} \models \varphi_{Conn} \iff \mathcal{G} \text{ ist zusammenhängend.} \quad (3.9)$$

*Idee:* Nutze den Satz  $\varphi_{Conn}$ , um einen FO[ $\{\leq\}$ ]-Satz  $\psi$  zu konstruieren, so dass für jede endliche lineare Ordnung  $\mathcal{B} = (B, \leq^{\mathcal{B}})$  mit  $|B| \geq 2$  gilt:

$$\mathcal{B} \models \psi \iff |B| \text{ ist gerade.}$$

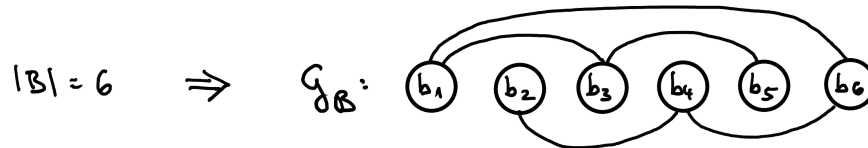
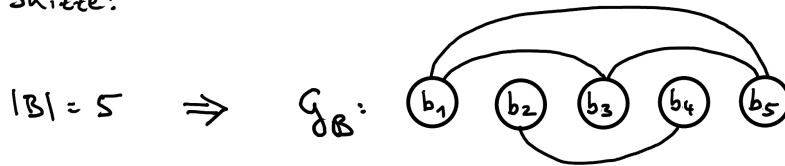
Von Bemerkung 3.57 wissen wir, dass es einen solchen Satz  $\psi$  nicht geben kann.

Um den Satz  $\psi$  zu konstruieren, ordnen wir jeder endlichen linearen Ordnung  $\mathcal{B} = (B, \leq^{\mathcal{B}})$  mit  $B = \{b_1, \dots, b_n\}$  und  $b_1 <^{\mathcal{B}} b_2 <^{\mathcal{B}} \dots <^{\mathcal{B}} b_n$  für  $n := |B| \geq 2$  den Graphen  $\mathcal{G}_{\mathcal{B}}$  mit Knotenmenge  $B$  zu, dessen Kantenmenge aus genau den Kanten zwischen  $b_i$  und  $b_{i+2}$ , für alle  $i \leq n-2$ , und einer zusätzlichen Kante zwischen  $b_1$  und  $b_n$  besteht.

---

<sup>4</sup>d.h.  $A = V^{\mathcal{G}}$  und  $E^{\mathcal{A}} = \{(u, v) : \{u, v\} \in E^{\mathcal{G}}\}$

Skizze:



Man sieht leicht, dass Folgendes gilt:

$$\mathcal{G}_B \text{ ist zusammenhängend} \iff |B| \text{ ist gerade.} \quad (3.10)$$

Sei nun  $\xi_E(x, y)$  eine  $\text{FO}\{\{\leq\}\}$ -Formel, die besagt:

- „ $y = x+2$ “ oder „ $x = y+2$ “ oder
- „ $x$  ist das kleinste und  $y$  ist das größte Element bzgl.  $\leq$ “ oder
- „ $x$  ist das größte und  $y$  ist das kleinste Element bzgl.  $\leq$ “.

Klar: Eine solche  $\text{FO}\{\{\leq\}\}$ -Formel  $\xi_E(x, y)$  lässt sich leicht formulieren (Details: Übung).

Ausgewertet in einer linearen Ordnung  $\mathcal{B}$  „simuliert“ die Formel  $\xi_E(x, y)$  gewissermaßen die Kantenrelation des Graphen  $\mathcal{G}_B$ .

Sei nun  $\psi$  der  $\text{FO}\{\{\leq\}\}$ -Satz, der aus dem  $\text{FO}\{\{E\}\}$ -Satz  $\varphi_{\text{Conn}}$  entsteht, indem jedes Atom der Form  $E(z_1, z_2)$  durch die  $\text{FO}\{\{\leq\}\}$ -Formel  $\xi_E(z_1, z_2)$  ersetzt wird.

Der Satz  $\psi$  ist also gerade so konstruiert, dass beim Auswerten von  $\psi$  in  $\mathcal{B}$  die Auswertung von  $\varphi_{\text{Conn}}$  in der zu  $\mathcal{G}_B$  gehörenden  $\sigma$ -Struktur  $\mathcal{A}$  simuliert wird. Es gilt also für jede endliche lineare Ordnung  $\mathcal{B}$  mit  $|B| \geq 2$ , den ungerichteten endlichen Graphen  $\mathcal{G}_B$  und die zugehörige  $\sigma$ -Struktur  $\mathcal{A}$ :

$$\begin{aligned} \mathcal{B} \models \psi &\iff \mathcal{A} \models \varphi_{\text{Conn}} \\ &\stackrel{(3.9)}{\iff} \mathcal{G}_B \text{ ist zusammenhängend} \\ &\stackrel{(3.10)}{\iff} |B| \text{ ist gerade.} \end{aligned}$$

Aber dies ist ein Widerspruch zu Bemerkung 3.57.

Somit muss unsere Annahme, dass der Satz  $\varphi_{Conn}$  existiert, falsch gewesen sein. Dies beendet den Beweis von (a).

Folie 274

(b) folgt direkt aus (a), denn:

Angenommen  $\varphi_{Reach}(x, y)$  wäre eine FO[ $\sigma$ ]-Formel, so dass für alle gerichteten Graphen  $\mathcal{A} = (A, E^{\mathcal{A}})$  und alle Knoten  $a, b \in A$  gilt:

$\mathcal{A} \models \varphi_{Reach}[a, b] \iff$  es gibt in  $\mathcal{A}$  einen Weg von Knoten  $a$  zu Knoten  $b$ .

Dann ist

$$\varphi_{Conn} := \forall x \forall y \varphi_{Reach}(x, y)$$

ein FO[ $\sigma$ ]-Satz, der in einem gerichteten Graphen  $\mathcal{A}$  genau dann erfüllt ist, wenn  $\mathcal{A}$  stark zusammenhängend ist.

Insbesondere gilt dann für jeden ungerichteten Graphen  $\mathcal{G}$  und die zu  $\mathcal{G}$  gehörende  $\sigma$ -Struktur  $\mathcal{A}$ :  $\mathcal{A} \models \varphi_{Conn} \iff \mathcal{G}$  ist zusammenhängend.

Dies ist ein Widerspruch zu (a).

□

Folie 275

## Logische Reduktionen

### Bemerkung 3.59.

Die im Beweis von Satz 3.58 benutzte Vorgehensweise ist unter dem Begriff *logische Reduktion* (oder *Transduktionen*) bekannt.

Im Beweis von Teil (b) wurde gezeigt: Falls es eine FO[ $\{E\}$ ]-Formel gibt, die ausdrückt, dass Knoten  $y$  von Knoten  $x$  aus erreichbar ist, dann gibt es auch eine FO[ $\{E\}$ ]-Formel, die Graph-Zusammenhang definiert.

Somit wurde das Problem, einen FO[ $\{E\}$ ]-Satz zu finden, der Graph-Zusammenhang definiert, auf das Problem reduziert, eine FO[ $\{E\}$ ]-Formel zu finden, die ausdrückt, dass Knoten  $y$  von Knoten  $x$  aus erreichbar ist.

Folie 276

Im Beweis von Teil (a) wurde das Problem, einen FO[ $\{\leq\}$ ]-Satz zu finden, der ausdrückt, dass eine endliche lineare Ordnung eine *gerade* Kardinalität besitzt, auf das Problem reduziert, einen FO[ $\{E\}$ ]-Satz zu finden, der Graph-Zusammenhang definiert.

D.h. es wurde gezeigt: Falls Graph-Zusammenhang FO-definierbar ist, so ist auch die Aussage „eine endliche lineare Ordnung besitzt eine *gerade* Kardinalität“ FO-definierbar.

Dies wurde dadurch erreicht, dass man innerhalb einer linearen Ordnung einen geeigneten Graphen „simuliert“ (bzw. „interpretiert“), indem man die Kantenrelation des Graphen durch eine  $\text{FO}\{\{\leq\}\}$ -Formel beschreibt.

Generell ist diese Methode der *logischen Reduktionen* oft nützlich, um bereits bekannte Nicht-Definierbarkeits-Resultate auf neue Nicht-Definierbarkeits-Resultate zu übertragen.

### 3.9 Erfüllbarkeit, Allgemeingültigkeit und die Folgerungsbeziehung

Folie 277

Die im Folgenden eingeführten Begriffe der Erfüllbarkeit, Allgemeingültigkeit und der Folgerungsbeziehung sind für die Logik erster Stufe ähnlich definiert wie für die Aussagenlogik.

Im Folgenden sei  $\sigma$  stets eine beliebige Signatur.

Folie 278

#### Erfüllbarkeit und Allgemeingültigkeit

**Definition 3.60.** Eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  (bzw. eine Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$ ) heißt *erfüllbar*, wenn es eine  $\sigma$ -Interpretation gibt, die  $\varphi$  (bzw.  $\Phi$ ) erfüllt.

Eine Formel oder Formelmenge, die *nicht erfüllbar* ist, nennen wir *unerfüllbar*.

**Definition 3.61.** Eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  heißt *allgemeingültig*, wenn *jede*  $\sigma$ -Interpretation die Formel  $\varphi$  erfüllt.

Wir schreiben kurz  $\models \varphi$  um auszudrücken, dass  $\varphi$  allgemeingültig ist.

Offensichtlicherweise gilt für alle  $\text{FO}[\sigma]$ -Formeln  $\varphi$ :

$$\varphi \text{ ist allgemeingültig} \iff \neg\varphi \text{ ist unerfüllbar.}$$

Folie 279

## Verum ( $\top$ ) und Falsum ( $\perp$ )

*Beispiele:*

- Die FO[ $\sigma$ ]-Formel  $\forall v_0 v_0=v_0$  ist allgemeingültig.
- Die FO[ $\sigma$ ]-Formel  $\exists v_0 \neg v_0=v_0$  ist unerfüllbar.

### Notation 3.62.

Wir schreiben  $\top$  (in Worten: *Verum*), um die allgemeingültige FO-Formel  $\forall v_0 v_0=v_0$  zu bezeichnen.

Wir schreiben  $\perp$  (in Worten: *Falsum*), um die unerfüllbare FO-Formel  $\exists v_0 \neg v_0=v_0$  zu bezeichnen.

Folie 280

## Die Folgerungsbeziehung

**Definition 3.63.** Eine FO[ $\sigma$ ]-Formel  $\psi$  *folgt* aus einer Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  (wir schreiben:  $\Phi \models \psi$ ), wenn für jede  $\sigma$ -Interpretation  $\mathcal{I}$  gilt: Falls  $\mathcal{I} \models \Phi$ , so gilt auch  $\mathcal{I} \models \psi$ .

**Notation.** Für zwei FO[ $\sigma$ ]-Formeln  $\varphi, \psi$  schreiben wir kurz  $\varphi \models \psi$  an Stelle von  $\{\varphi\} \models \psi$  und sagen, dass die Formel  $\psi$  aus der Formel  $\varphi$  folgt.

Folie 281

## Zusammenhänge

Es bestehen ähnliche Zusammenhänge wie bei der Aussagenlogik:

**Lemma 3.64** (Allgemeingültigkeit, Unerfüllbarkeit und Folgerung).

Für jede FO[ $\sigma$ ]-Formel  $\varphi$  gilt:

$$(a) \quad \varphi \text{ ist allgemeingültig} \iff \varphi \equiv \top \iff \top \models \varphi.$$

$$(b) \quad \varphi \text{ ist unerfüllbar} \iff \varphi \equiv \perp \iff \varphi \models \perp.$$

$$(c) \quad \models \varphi \iff \emptyset \models \varphi.$$

*D.h.:*  $\varphi$  ist allgemeingültig  $\iff \varphi$  folgt aus der leeren Menge.

**Lemma 3.65** (Erfüllbarkeit und die Folgerungsbeziehung).

(a) Für alle Formelmengen  $\Phi \subseteq \text{FO}[\sigma]$  und alle  $\text{FO}[\sigma]$ -Formeln  $\psi$  gilt:

$$\Phi \models \psi \iff \Phi \cup \{\neg\psi\} \text{ ist unerfüllbar.}$$

(b) Für alle  $\text{FO}[\sigma]$ -Formeln  $\varphi, \psi$  gilt:  $\varphi \equiv \psi \iff \models (\varphi \leftrightarrow \psi)$ .

Beweis der beiden Lemmas: Analog zu den Beweisen der entsprechenden Resultate in der Aussagenlogik. Details: Übung.

### 3.10 Normalformen

Folie 282

#### Negationsnormalform

Die *Negationsnormalform* für Formeln der Logik erster Stufe ist ähnlich definiert wie die Negationsnormalform der Aussagenlogik.

**Definition 3.66.** Sei  $\sigma$  eine beliebige Signatur.

Eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  ist in *Negationsnormalform* (kurz: *NNF*), wenn Negationszeichen in  $\varphi$  nur unmittelbar vor atomaren Subformeln auftreten und  $\varphi$  den Junktor „ $\rightarrow$ “ nicht enthält.

**Satz 3.67.** Jede  $\text{FO}[\sigma]$ -Formel  $\varphi$  ist äquivalent zu einer Formel in *NNF*.

*Beweis.* Gemäß Satz 3.46 können wir o.B.d.A. annehmen, dass  $\varphi$  den Junktor „ $\rightarrow$ “ nicht enthält.

Ähnlich wie für die Aussagenlogik definieren wir per Induktion über den Aufbau zu jeder  $\text{FO}[\sigma]$ -Formel  $\varphi$  zwei  $\text{FO}[\sigma]$ -Formeln  $\varphi'$  und  $\varphi''$  in *NNF*, so dass gilt:  $\varphi \equiv \varphi'$  und  $\neg\varphi \equiv \varphi''$ .

Details: Übung. □

Folie 283

## Pränexe Normalform

**Definition 3.68.** Sei  $\sigma$  eine beliebige Signatur.

- (a) Eine  $\text{FO}[\sigma]$ -Formel heißt *quantorenfrei*, falls in ihr keins der Symbole  $\exists, \forall$  vorkommt.

Die Menge aller quantorenfreien  $\text{FO}[\sigma]$ -Formeln bezeichnen wir mit  $\text{QF}_\sigma$ .

- (b) Eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  ist in *pränexer Normalform* (bzw. *Pränex-Normalform*, kurz: *PNF*), wenn sie von der Form

$$Q_1 x_1 \cdots Q_n x_n \chi$$

ist, wobei  $n \geq 0$ ,  $Q_1, \dots, Q_n \in \{\exists, \forall\}$ ,  $x_1, \dots, x_n \in \text{VAR}$  und  $\chi \in \text{QF}_\sigma$ .

$Q_1 x_1 \cdots Q_n x_n$  wird *Quantoren-Präfix* von  $\varphi$  genannt;

$\chi$  heißt *Kern* (bzw. *Matrix*) von  $\varphi$ .

**Satz 3.69.** Jede  $\text{FO}[\sigma]$ -Formel  $\varphi$  ist äquivalent zu einer  $\text{FO}[\sigma]$ -Formel  $\varphi'$  in pränexer Normalform mit  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

Folie 284

Bevor wir Satz 3.69 beweisen, betrachten wir zunächst ein Beispiel.

**Beispiel 3.70.** Sei

$$\varphi(y) := \forall x \neg (\exists y E(x, y) \rightarrow \exists x E(x, y)).$$

Umformung in eine äquivalente Formel in Pränex-Normalform:

$\varphi \equiv \forall x \neg (\neg \exists y E(x, y) \vee \exists x E(x, y))$	Elimination von “ $\rightarrow$ ”
$\equiv \forall x \neg (\forall y \neg E(x, y) \vee \exists x E(x, y))$	$\neg \exists y \psi \equiv \forall y \neg \psi$
$\equiv \forall x \neg (\forall z_1 \neg E(x, z_1) \vee \exists z_2 E(z_2, y))$	Umbenennung von gebundenen Variablen
$\equiv \forall x \neg \forall z_1 \exists z_2 (\neg E(x, z_1) \vee E(z_2, y))$	Zusammenlegung der Disjunktion
$\equiv \forall x \exists z_1 \forall z_2 \neg (\neg E(x, z_1) \vee E(z_2, y))$	Negation

Diese Formel ist in PNF.

Folie 285



**Beweis von Satz 3.69:**

Wir zeigen zunächst drei Lemmas und schließen danach den Beweis ab.

**Lemma 3.71.**

Sei  $\psi := Q_1x_1 \cdots Q_nx_n \chi$ , wobei  $n \geq 0$ ,  $Q_1, \dots, Q_n \in \{\exists, \forall\}$  und  $\chi \in \text{FO}[\sigma]$ . Für jedes  $Q \in \{\exists, \forall\}$  sei

$$\tilde{Q} := \begin{cases} \forall & \text{falls } Q = \exists, \\ \exists & \text{falls } Q = \forall. \end{cases}$$

Dann gilt:  $\neg\psi \equiv \tilde{Q}_1x_1 \cdots \tilde{Q}_nx_n \neg\chi$ .

*Beweis.* Einfaches Nachrechnen per Induktion nach  $n$  unter Verwendung der Tatsache, dass  $\neg\exists x \varphi \equiv \forall x \neg\varphi$  und  $\neg\forall x \varphi \equiv \exists x \neg\varphi$  (Lemma 3.44). Details: Übung. □

Folie 286

**Lemma 3.72.** Für alle FO[ $\sigma$ ]-Formeln  $\varphi$  und  $\psi$  und für alle Variablen  $x \in \text{VAR} \setminus \text{frei}(\varphi)$  gilt:

$$\begin{aligned} (\varphi \wedge \exists x \psi) &\equiv \exists x (\varphi \wedge \psi) & , & & (\varphi \wedge \forall x \psi) &\equiv \forall x (\varphi \wedge \psi) , \\ (\varphi \vee \exists x \psi) &\equiv \exists x (\varphi \vee \psi) & , & & (\varphi \vee \forall x \psi) &\equiv \forall x (\varphi \vee \psi) . \end{aligned}$$

*Beweis.* Die Beweise aller vier Äquivalenzen sind ähnlich. Wir beweisen hier nur die erste:

$$(\varphi \wedge \exists x \psi) \equiv \exists x (\varphi \wedge \psi) . \tag{3.11}$$

„ $\implies$ “: Sei  $\mathcal{I} = (\mathcal{A}, \beta)$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models (\varphi \wedge \exists x \psi)$ .

Dann gilt:  $\mathcal{I} \models \varphi$  und  $\mathcal{I} \models \exists x \psi$ . Insbesondere gibt es ein  $a \in A$ , so dass  $\mathcal{I}_x^a \models \psi$ .

Wegen  $\mathcal{I} \models \varphi$  und  $x \notin \text{frei}(\varphi)$  folgt aus dem Koinzidenzlemma, dass auch  $\mathcal{I}_x^a \models \varphi$ .

Somit gilt:  $\mathcal{I}_x^a \models (\varphi \wedge \psi)$ , und daher gilt:  $\mathcal{I} \models \exists x (\varphi \wedge \psi)$ .

„ $\Leftarrow$ “: Sei  $\mathcal{I} = (\mathcal{A}, \beta)$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \exists x (\varphi \wedge \psi)$ .

Somit gibt es ein  $a \in A$ , so dass  $\mathcal{I}_x^a \models (\varphi \wedge \psi)$ .

Insbesondere gilt:  $\mathcal{I}_x^a \models \varphi$ . Wegen  $x \notin \text{frei}(\varphi)$  folgt gemäß Koinzidenzlemma, dass  $\mathcal{I} \models \varphi$ .

Außerdem gilt wegen  $\mathcal{I}_x^a \models \psi$ , dass  $\mathcal{I} \models \exists x \psi$ .

Insgesamt gilt also:  $\mathcal{I} \models (\varphi \wedge \exists x \psi)$ .

Dies beendet den Beweis von (3.11). Die anderen drei im Lemma genannten Äquivalenzen können auf analoge Art bewiesen werden. Details: Übung.  $\square$

Folie 287

**Lemma 3.73.** *Seien*

$$\psi_1 := Q_1 x_1 \cdots Q_\ell x_\ell \chi_1 \quad \text{und} \quad \psi_2 := Q'_1 y_1 \cdots Q'_m y_m \chi_2,$$

wobei  $\ell, m \geq 0$ ,  $Q_1, \dots, Q_\ell, Q'_1, \dots, Q'_m \in \{\exists, \forall\}$ ,  
 $x_1, \dots, x_\ell, y_1, \dots, y_m \in \text{VAR}$ ,  $\chi_1, \chi_2 \in \text{FO}[\sigma]$ .

Es gelte:  $\{x_1, \dots, x_\ell\} \cap \text{frei}(\psi_2) = \emptyset$  und  $\{y_1, \dots, y_m\} \cap \text{frei}(\chi_1) = \emptyset$ .

Dann gilt für  $* \in \{\wedge, \vee\}$ , dass

$$(\psi_1 * \psi_2) \equiv Q_1 x_1 \cdots Q_\ell x_\ell Q'_1 y_1 \cdots Q'_m y_m (\chi_1 * \chi_2).$$

*Beweis.* Zwei Induktionen über  $\ell$  bzw.  $m$  unter Verwendung von Lemma 3.72:

Per Induktion nach  $\ell$  folgt unter Verwendung von Lemma 3.72, dass

$$(\psi_2 * Q_1 x_1 \cdots Q_\ell x_\ell \chi_1) \equiv Q_1 x_1 \cdots Q_\ell x_\ell (\psi_2 * \chi_1).$$

Die Kommutativität von  $* \in \{\wedge, \vee\}$  liefert daher:

$$(\psi_1 * \psi_2) \equiv Q_1 x_1 \cdots Q_\ell x_\ell (\chi_1 * \psi_2). \quad (3.12)$$

Andererseits folgt per Induktion nach  $m$  unter Verwendung von Lemma 3.72, dass

$$(\chi_1 * Q'_1 y_1 \cdots Q'_m y_m \chi_2) \equiv Q'_1 y_1 \cdots Q'_m y_m (\chi_1 * \chi_2). \quad (3.13)$$

Die Kombination von (3.12) und (3.13) liefert also:

$$(\psi_1 * \psi_2) \equiv Q_1 x_1 \cdots Q_\ell x_\ell Q'_1 y_1 \cdots Q'_m y_m (\chi_1 * \chi_2).$$

$\square$

Folie 288

### Abschluss des Beweises von Satz 3.69:

Sei  $\varphi$  eine  $\text{FO}[\sigma]$ -Formel. Gemäß Satz 3.46 können wir o.B.d.A. annehmen, dass  $\varphi$  den Junktor „ $\rightarrow$ “ nicht enthält.

Per Induktion über den Aufbau von  $\varphi$  zeigen wir, dass es eine zu  $\varphi$  äquivalente Formel  $\varphi'$  in PNF gibt mit  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

*Induktionsanfang:* Atomare Formeln sind quantorenfrei und daher insbesondere in PNF.

*Induktionsschritt:*

Fall 1:  $\varphi$  ist von der Form  $Qx\psi$  mit  $Q \in \{\exists, \forall\}$ ,  $x \in \text{VAR}$ ,  $\psi \in \text{FO}[\sigma]$ :

Gemäß Induktionsannahme gibt es eine zu  $\psi$  äquivalente Formel  $\psi'$  in PNF mit  $\text{frei}(\psi') = \text{frei}(\psi)$ .

Offensichtlich ist  $\varphi' := Qx\psi'$  die gesuchte PNF-Formel mit  $\varphi' \equiv \varphi$ .

Es gilt:  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

Fall 2:  $\varphi$  ist von der Form  $\neg\psi$  mit  $\psi \in \text{FO}[\sigma]$ .

Gemäß Induktionsannahme gibt es eine zu  $\psi$  äquivalente Formel  $\psi'$  in PNF mit  $\text{frei}(\psi') = \text{frei}(\psi)$ .

Klar:  $\varphi \equiv \neg\psi'$ .

Wir nutzen Lemma 3.71 und erhalten die zu  $\neg\psi'$  äquivalente Formel  $\varphi'$  in PNF. Es gilt:  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

Fall 3:  $\varphi$  ist von der Form  $(\psi_1 * \psi_2)$  mit  $* \in \{\wedge, \vee\}$  und  $\psi_1, \psi_2 \in \text{FO}[\sigma]$ .

Gemäß Induktionsannahme gibt es Formeln  $\psi'_1, \psi'_2$  in PNF, so dass für jedes  $i \in \{1, 2\}$  gilt:  $\psi'_i \equiv \psi_i$  und  $\text{frei}(\psi'_i) = \text{frei}(\psi_i)$ .

Klar:  $\varphi \equiv (\psi'_1 * \psi'_2)$ .

Sei  $Q_1x_1 \cdots Q_\ell x_\ell \chi_1$  die Form von  $\psi'_1$  (mit  $\chi_1$  quantorenfrei) und sei

$Q'_1y_1 \cdots Q'_my_m \chi_2$  die Form von  $\psi'_2$  (mit  $\chi_2$  quantorenfrei).

Wir können o.B.d.A. annehmen, dass  $\{x_1, \dots, x_\ell\} \cap \text{frei}(\psi_2) = \emptyset$  und

$\{y_1, \dots, y_m\} \cap \text{frei}(\chi_1) = \emptyset$  (dies können wir durch konsistentes

Umbenennen der in  $\psi'_1$  bzw.  $\psi'_2$  gebundenen Variablen  $x_1, \dots, x_\ell, y_1, \dots, y_m$  erreichen).

Lemma 3.73 liefert uns dann die gesuchte zu  $(\psi'_1 * \psi'_2)$  äquivalente Formel  $\varphi'$  in PNF. Es gilt:  $\text{frei}(\varphi') = \text{frei}(\varphi)$ .

Dies beendet den Beweis von Satz 3.69. □



## *Kapitel 4*

# Grundlagen des automatischen Schließens

Folie 289

### **Ziel: Automatisches Schließen**

- In typischen Anwendungen der Logik beschreibt man mit Hilfe einer Formelmenge das Wissen über ein Anwendungsszenario und will aus diesem Wissen dann, möglichst automatisch, Folgerungen ziehen.
- In diesem Kapitel werden wir untersuchen, inwieweit sich für die Logik erster Stufe das Folgern automatisieren lässt.
- Wir werden einen syntaktischen Beweisbegriff einführen, der genau dem semantischen Folgerungsbegriff entspricht (*Vollständigkeitssatz*).
- Dadurch werden wir einen Algorithmus erhalten, der nach und nach alle allgemeingültigen Sätze der Logik erster Stufe aufzählt.
- Andererseits werden wir zeigen, dass es keinen Algorithmus gibt, der bei Eingabe eines beliebigen Satzes der Logik erster Stufe entscheidet, ob der Satz allgemeingültig ist.
- Als Folgerung aus dem Vollständigkeitssatz werden wir auch den *Endlichkeitssatz* für die Logik erster Stufe erhalten.

## 4.1 Kalküle und Ableitungen

Folie 290

### Ableitungsregeln und Kalküle

**Definition 4.1.** Sei  $M$  eine beliebige Menge.

(a) Eine *Ableitungsregel über  $M$*  (kurz: *Regel*) hat die Form

$$\frac{a_1 \cdots a_n}{b}$$

wobei  $n \geq 0$  und  $a_1, \dots, a_n, b \in M$ .

Wir bezeichnen  $a_1, \dots, a_n$  als die *Voraussetzungen* der Regel und  $b$  als die *Konsequenz*.

Ableitungsregeln ohne Voraussetzungen (also mit  $n = 0$ ) bezeichnen wir als *Axiome*.

(b) Ein *Kalkül über  $M$*  ist eine Menge von Ableitungsregeln über  $M$ .

Folie 291

### Ableitungen

**Definition 4.2.**

Sei  $\mathfrak{K}$  ein Kalkül über einer Menge  $M$ , sei  $V \subseteq M$  und sei  $a \in M$ .

(a) Eine *Ableitung von  $a$  aus  $V$  in  $\mathfrak{K}$*  ist eine endliche Folge  $(a_1, \dots, a_\ell) \in M^\ell$ , so dass  $\ell \geq 1$ ,  $a_\ell = a$  und für alle  $i \in \{1, \dots, \ell\}$  gilt:<sup>1</sup>

- $a_i \in V$  oder
- $\frac{\quad}{a_i}$  ist ein Axiom in  $\mathfrak{K}$  oder
- es gibt in  $\mathfrak{K}$  eine Ableitungsregel

$$\frac{b_1 \cdots b_n}{a_i}$$

so dass  $b_1, \dots, b_n \in \{a_1, \dots, a_{i-1}\}$ .

---

<sup>1</sup>Die Menge  $V$  kann hierbei als Menge von „Voraussetzungen“ betrachtet werden, und der Kalkül legt fest, welche Axiome gelten und welche Schlussweisen zulässig sind.

Der besseren Lesbarkeit halber schreiben wir in konkreten Beispielen Ableitungen der Form  $(a_1, \dots, a_\ell)$  oft zeilenweise, also

(1)  $a_1$   
(2)  $a_2$   
 $\vdots$   
( $\ell$ )  $a_\ell$

und geben am Ende jeder Zeile eine kurze Begründung an.

Folie 292

- (b) Ein Element  $a \in M$  ist *aus  $V$  in  $\mathfrak{K}$  ableitbar*, wenn es eine Ableitung von  $a$  aus  $V$  in  $\mathfrak{K}$  gibt.
- (c) Wir schreiben  $\text{abl}_{\mathfrak{K}}(V)$ , um die Menge aller aus  $V$  in  $\mathfrak{K}$  ableitbaren Elemente zu bezeichnen.
- (d) Für  $V = \emptyset$  nutzen wir folgende Notationen:

Eine *Ableitung von  $a$  in  $\mathfrak{K}$*  ist eine Ableitung von  $a$  aus  $\emptyset$  in  $\mathfrak{K}$ .

Ein Element  $a \in M$  heißt *ableitbar aus  $\mathfrak{K}$* , falls es eine Ableitung von  $a$  in  $\mathfrak{K}$  gibt.

Die Menge aller in  $\mathfrak{K}$  ableitbaren Elemente bezeichnen wir mit  $\text{abl}_{\mathfrak{K}}$ , d.h.:  $\text{abl}_{\mathfrak{K}} := \text{abl}_{\mathfrak{K}}(\emptyset)$ .

Folie 293

Wir werden Kalküle nutzen, um auf elegante Art *rekursive Definitionen* bestimmter Mengen anzugeben:

Um eine bestimmte Teilmenge  $A$  einer Menge  $M$  rekursiv zu definieren, genügt es, einen Kalkül  $\mathfrak{K}$  über  $M$  anzugeben, für den gilt:  $\text{abl}_{\mathfrak{K}} = A$ .

Folie 294

### Beispiel: Mengen natürlicher Zahlen

#### Beispiel 4.3.

Sei  $\mathfrak{K}$  der Kalkül über  $M := \mathbb{N}$  mit folgenden Ableitungsregeln:

- Axiom:  $\overline{1}$
- Weitere Regeln:  $\frac{n}{2n}$ , für jedes  $n \in \mathbb{N}$ .

*Fragen:*

- Was ist  $\text{abl}_{\mathfrak{K}}$ ?
- Was ist  $\text{abl}_{\mathfrak{K}}(V)$  für  $V := \{3\}$ ?

*Antworten:*

- $\text{abl}_{\mathfrak{K}}$  ist die Menge aller Zweierpotenzen, d.h.  $\text{abl}_{\mathfrak{K}} = \{2^i : i \in \mathbb{N}\}$ .
- $\text{abl}_{\mathfrak{K}}(\{3\}) = \{2^i : i \in \mathbb{N}\} \cup \{2^i \cdot 3 : i \in \mathbb{N}\}$

Folie 295

### Beispiel: Aussagenlogik

#### Beispiel 4.4.

Sei  $\Sigma := A_{\text{AL}}$  das Alphabet der Aussagenlogik, d.h.

$$\Sigma = \text{AS} \cup \{ \neg, \wedge, \vee, \rightarrow, \mathbf{0}, \mathbf{1}, (, ) \},$$

wobei  $\text{AS} = \{A_i : i \in \mathbb{N}\}$  die Menge aller Aussagensymbole ist.

*Gesucht:* Ein Kalkül  $\mathfrak{K}$  über  $M := \Sigma^*$ , aus dem genau die syntaktisch korrekten aussagenlogischen Formeln ableitbar sind, d.h.  $\text{abl}_{\mathfrak{K}} = \text{AL}$ .

*Lösung:*  $\mathfrak{K}$  besteht aus folgenden Ableitungsregeln:

- Axiome:  $\overline{\mathbf{0}}$ ,  $\overline{\mathbf{1}}$ ,  $\overline{X}$ , für jedes Aussagensymbol  $X \in \text{AS}$ .
- Weitere Regeln: Für jedes  $\varphi \in \Sigma^*$  und jedes  $\psi \in \Sigma^*$  die Regeln

$$\frac{\varphi}{\neg\varphi}, \quad \frac{\varphi \quad \psi}{(\varphi \wedge \psi)}, \quad \frac{\varphi \quad \psi}{(\varphi \vee \psi)}, \quad \frac{\varphi \quad \psi}{(\varphi \rightarrow \psi)}$$

Dann gilt:  $\text{abl}_{\mathfrak{K}} = \text{AL}$ .

Folie 296



## Beispiel: Resolution

Die Kalkül-Schreibweise lässt sich auch dazu nutzen, eine elegante Darstellung der in Kapitel 2.6 eingeführten *Resolutionswiderlegungen* zu angeben.

*Zur Erinnerung:*

- Eine *Klausel* ist eine endliche Menge von Literalen.  
Ein *Literal* ist eine aussagenlogische Formel der Form  $X$  oder  $\neg X$ , wobei  $X \in \text{AS}$ .
- Wir haben in Satz 2.59 gezeigt, dass für jede Menge  $\Gamma$  von Klauseln gilt:

$$\Gamma \text{ ist unerfüllbar} \iff \Gamma \vdash_R \emptyset.$$

Hierbei ist  $\emptyset$  die *leere Klausel*.

„ $\Gamma \vdash_R \emptyset$ “ bedeutet, dass es eine *Resolutionswiderlegung* von  $\Gamma$  gibt.

Zur Erinnerung hier die Definition des Begriffs der Resolutionswiderlegungen:

Folie 297

## Resolutionsableitungen und -widerlegungen

**Definition 2.56.** Sei  $\Gamma$  eine Klauselmenge.

- (a) Eine *Resolutionsableitung* einer Klausel  $\delta$  aus  $\Gamma$  ist ein Tupel  $(\delta_1, \dots, \delta_\ell)$  von Klauseln, so dass gilt:  $\ell \geq 1$ ,  $\delta_\ell = \delta$ , und für alle  $i \in [\ell]$  ist
- $\delta_i \in \Gamma$ , oder
  - es gibt  $j, k \in [i-1]$ , so dass  $\delta_i$  eine Resolvente von  $\delta_j$  und  $\delta_k$  ist.
- (b) Eine *Resolutionswiderlegung* von  $\Gamma$  ist eine Resolutionsableitung der leeren Klausel aus  $\Gamma$ .

*Zur Erinnerung:*

Eine Klausel  $\delta$  ist genau dann eine *Resolvente* zweier Klauseln  $\gamma_1$  und  $\gamma_2$ , wenn es ein Literal  $\lambda$  gibt, so dass gilt:

$$\lambda \in \gamma_1, \quad \bar{\lambda} \in \gamma_2 \quad \text{und} \quad \delta = (\gamma_1 \setminus \{\lambda\}) \cup (\gamma_2 \setminus \{\bar{\lambda}\}).$$

Folie 298

## Der Resolutionskalkül der Aussagenlogik

*Gesucht:* Ein Kalkül  $\mathfrak{K}_R$  über der Menge aller Klauseln, so dass für jede Klauselmenge  $\Gamma$  und jede Klausel  $\delta$  gilt:

$$\delta \in \text{abl}_{\mathfrak{K}_R}(\Gamma) \iff \Gamma \vdash_R \delta$$

d.h.:  $\delta$  ist genau dann aus  $\Gamma$  in  $\mathfrak{K}_R$  ableitbar, wenn es eine Resolutionsableitung von  $\delta$  aus  $\Gamma$  gibt.

*Lösung:*  $\mathfrak{K}_R$  besteht aus folgenden Ableitungsregeln:

Für alle Klauseln  $\gamma_1$  und  $\gamma_2$ , für jedes Literal  $\lambda$ , so dass  $\lambda \in \gamma_1$  und  $\bar{\lambda} \in \gamma_2$ , und für die Klausel  $\delta := (\gamma_1 \setminus \{\lambda\}) \cup (\gamma_2 \setminus \{\bar{\lambda}\})$  enthält  $\mathfrak{K}_R$  die Ableitungsregel

$$\frac{\gamma_1 \quad \gamma_2}{\delta}$$

Dann entsprechen Ableitungen in  $\mathfrak{K}_R$  aus einer Klauselmenge  $\Gamma$  gerade den Resolutionsableitungen aus  $\Gamma$ , und somit gilt:  $\text{abl}_{\mathfrak{K}}(\Gamma) = \{\delta : \Gamma \vdash_R \delta\}$ . Insbesondere gibt es genau dann eine Resolutionswiderlegung von  $\Gamma$ , wenn  $\text{abl}_{\mathfrak{K}}(\Gamma)$  die leere Klausel enthält.

Folie 299

Der Kalkül  $\mathfrak{K}_R$  wird *Resolutionskalkül der Aussagenlogik* genannt.

Folie 300

## Kalküle und abgeschlossene Mengen

**Definition 4.5.** Sei  $\mathfrak{K}$  ein Kalkül über einer Menge  $M$ .

Eine Menge  $A \subseteq M$  heißt *abgeschlossen unter  $\mathfrak{K}$* , wenn für jede Ableitungsregel

$$\frac{a_1 \cdots a_n}{b}$$

in  $\mathfrak{K}$  gilt: Falls  $a_1, \dots, a_n \in A$ , so ist auch  $b \in A$ .

**Satz 4.6.** Sei  $\mathfrak{K}$  ein Kalkül über einer Menge  $M$  und sei  $V \subseteq M$ .

Dann ist  $\text{abl}_{\mathfrak{K}}(V)$  die bzgl. „ $\subseteq$ “ kleinste unter  $\mathfrak{K}$  abgeschlossene Menge, die  $V$  enthält. D.h. es gilt:

(a)  $V \subseteq \text{abl}_{\mathfrak{K}}(V)$ .

(b)  $\text{abl}_{\mathfrak{K}}(V)$  ist abgeschlossen unter  $\mathfrak{K}$ .

(c) Für jede Menge  $A$  mit  $V \subseteq A \subseteq M$  gilt:  
 Falls  $A$  abgeschlossen ist unter  $\mathfrak{K}$ , so ist  $\text{abl}_{\mathfrak{K}}(V) \subseteq A$ .

$$(d) \text{abl}_{\mathfrak{K}}(V) = \bigcap_{\substack{V \subseteq A \subseteq M, \\ A \text{ abgeschlossen unter } \mathfrak{K}}} A.$$

*Beweis.*

(a) Für jedes  $v \in V$  ist  $(v)$  eine Ableitung von  $v$  aus  $V$  in  $\mathfrak{K}$ . Somit ist  $V \subseteq \text{abl}_{\mathfrak{K}}(V)$ .

(b) Sei

$$\frac{a_1 \cdots a_n}{b}$$

eine Ableitungsregel in  $\mathfrak{K}$ , so dass  $a_1, \dots, a_n \in \text{abl}_{\mathfrak{K}}(V)$ . Wir müssen zeigen, dass dann gilt:  $b \in \text{abl}_{\mathfrak{K}}(V)$ . D.h. wir müssen eine Ableitung von  $b$  aus  $V$  in  $\mathfrak{K}$  finden.

Laut Voraussetzung gilt für jedes  $i \in [n]$ :  
 $a_i \in \text{abl}_{\mathfrak{K}}(V)$ , d.h. es gibt eine Ableitung

$$(a_1^i, \dots, a_{\ell_i}^i)$$

von  $a_i$  aus  $V$  in  $\mathfrak{K}$ . Insbesondere gilt:  $a_i = a_{\ell_i}^i$ .

Dann ist

$$(a_1^1, \dots, a_{\ell_1}^1, a_1^2, \dots, a_{\ell_2}^2, \dots, a_1^n, \dots, a_{\ell_n}^n, b)$$

eine Ableitung von  $b$  aus  $V$  in  $\mathfrak{K}$ . Somit gilt:  $b \in \text{abl}_{\mathfrak{K}}(V)$ .

(c) Sei  $A$  eine Menge mit  $V \subseteq A \subseteq M$ , die abgeschlossen ist unter  $\mathfrak{K}$ . Wir müssen zeigen, dass gilt:  $\text{abl}_{\mathfrak{K}}(V) \subseteq A$ .

Sei dazu  $a$  ein beliebiges Element in  $\text{abl}_{\mathfrak{K}}(V)$ , und sei  $(a_1, \dots, a_\ell)$  eine Ableitung von  $a$  aus  $V$  in  $\mathfrak{K}$ . Wir wollen zeigen, dass gilt:  $a \in A$ .

Wir zeigen per Induktion nach  $i$ , dass für jedes  $i \in [n]$  gilt:  $a_i \in A$ .

Wegen  $a = a_\ell$  gilt dann insbesondere, dass  $a \in A$ .

*Induktionsanfang*  $i = 1$ :

Da  $(a_1, \dots, a_\ell)$  eine Ableitung von  $a$  aus  $V$  in  $\mathfrak{K}$  ist, gilt insbesondere:  
 $a_1 \in V$  oder  $\frac{\quad}{a_1}$  ist ein Axiom in  $\mathfrak{K}$ .

Im ersten Fall ist  $a_1 \in A$  wegen  $a_1 \in V \subseteq A$ .

Im zweiten Fall ist  $a_1 \in A$ , da  $A$  laut Voraussetzung unter  $\mathfrak{K}$  abgeschlossen ist.

*Induktionsschritt  $i-1 \rightarrow i$ :*

Die Induktionsannahme besagt, dass für jedes  $j \leq i-1$  gilt:  $a_j \in A$ .

Wir müssen im Induktionsschritt zeigen, dass auch gilt:  $a_i \in A$ .

Da  $(a_1, \dots, a_\ell)$  eine Ableitung von  $a$  aus  $V$  in  $\mathfrak{K}$  ist, gilt insbesondere:

$a_i \in V$  oder  $\frac{\quad}{a_i}$  ist ein Axiom in  $\mathfrak{K}$  oder es gibt in  $\mathfrak{K}$  eine

Ableitungsregel  $\frac{b_1 \cdots b_n}{a_i}$  so dass  $b_1, \dots, b_n \in \{a_1, \dots, a_{i-1}\}$  ist.

In den ersten beiden Fällen folgt „ $a_i \in A$ “ genauso wie im Induktionsanfang „ $a_1 \in A$ “ folgt.

Im dritten Fall liefert die Induktionsannahme, dass gilt:  $b_1, \dots, b_n \in A$ .

Da außerdem  $A$  laut Voraussetzung unter  $\mathfrak{K}$  abgeschlossen ist, folgt:  $a_i \in A$ .

(d) „ $\subseteq$ “ folgt direkt aus (c).

„ $\supseteq$ “ folgt direkt aus (a) und (b), da für die Menge  $A := \text{abl}_{\mathfrak{K}}(V)$  gemäß

(a) und (b) gilt:  $V \subseteq A \subseteq M$  und  $A$  ist abgeschlossen unter  $\mathfrak{K}$ .

Somit ist  $\text{abl}_{\mathfrak{K}}(V)$  eine der Mengen  $A$ , aus denen der Durchschnitt gebildet wird. Daher gilt:

$$\bigcap_{\substack{V \subseteq A \subseteq M, \\ A \text{ abgeschlossen unter } \mathfrak{K}}} A \subseteq \text{abl}_{\mathfrak{K}}(V).$$

□

### Induktionsprinzip für die ableitbaren Elemente eines Kalküls

Sei  $\mathfrak{K}$  ein Kalkül über einer Menge  $M$  und sei  $V \subseteq M$ . Um zu zeigen, dass eine bestimmte Aussage  $\mathbb{A}(a)$  für alle aus  $V$  in  $\mathfrak{K}$  ableitbaren Elemente  $a$  gilt, können wir das Induktionsprinzip nutzen und einfach Folgendes zeigen:

(1) Die Aussage  $\mathbb{A}(a)$  gilt für jedes  $a \in V$ , und

(2) für jede Ableitungsregel

$$\frac{a_1 \cdots a_n}{b}$$

in  $\mathfrak{K}$  gilt: Falls  $\mathbb{A}(a_i)$  für jedes  $i \in [n]$  gilt, so gilt auch  $\mathbb{A}(b)$ .

Daraus folgt laut dem nächsten Lemma dann, dass  $\mathbb{A}(a)$  für jedes  $a \in \text{abl}_{\mathfrak{K}}(V)$  gilt.

**Lemma 4.7.** *Sei  $\mathfrak{K}$  ein Kalkül über einer Menge  $M$  und sei  $V \subseteq M$ . Falls*

(1) *eine Aussage  $\mathbb{A}(a)$  für jedes  $a \in V$  gilt und*

(2) *für jede Ableitungsregel*

$$\frac{a_1 \cdots a_n}{b}$$

*in  $\mathfrak{K}$  gilt: falls  $\mathbb{A}(a_i)$  für jedes  $i \in [n]$  gilt, so gilt auch  $\mathbb{A}(b)$ ,*

*dann gilt die Aussage  $\mathbb{A}(a)$  für jedes  $a \in \text{abl}_{\mathfrak{K}}(V)$ .*

Folie 302

*Beweis.* Es seien (1) und (2) erfüllt.  
Betrachte die Menge

$$A := \{ a \in M : \text{die Aussage } \mathbb{A}(a) \text{ gilt} \} .$$

Wegen (1) ist  $V \subseteq A$ .

Wegen (2) ist  $A$  abgeschlossen unter  $\mathfrak{K}$ .

Aus Satz 4.6 folgt daher:  $\text{abl}_{\mathfrak{K}}(V) \subseteq A$ .

Somit gilt die Aussage  $\mathbb{A}(a)$  für jedes  $a \in \text{abl}_{\mathfrak{K}}(V)$ . □

## 4.2 Ein Beweiskalkül für die Logik erster Stufe — der Vollständigkeitssatz

Folie 303

### Notation

- In diesem Kapitel sei  $\sigma$  eine beliebige fest gewählte Signatur.
- Der Einfachheit halber werden wir o.B.d.A. in diesem Kapitel nur FO[ $\sigma$ ]-Formeln betrachten, in denen das Symbol „ $\rightarrow$ “ nicht vorkommt.
- $t, u, t_1, t_2, t', u', u'', \dots$  bezeichnen immer  $\sigma$ -Terme.
- $\varphi, \psi, \chi, \dots$  bezeichnen immer FO[ $\sigma$ ]-Formeln.

- $\Phi, \Psi, \Phi_1, \Phi_2, \Psi', \dots$  bezeichnen immer Mengen von  $\text{FO}[\sigma]$ -Formeln.
- $\Gamma, \Delta, \Gamma', \Delta_1, \Delta_2, \dots$  bezeichnen immer *endliche* Mengen von  $\text{FO}[\sigma]$ -Formeln.
- Für  $\Phi \subseteq \text{FO}[\sigma]$  ist  $\text{frei}(\Phi) := \bigcup_{\varphi \in \Phi} \text{frei}(\varphi)$ .  
Manchmal schreiben wir auch  $\text{frei}(\Phi, \varphi)$  an Stelle von  $\text{frei}(\Phi \cup \{\varphi\})$ .
- Ist  $M$  eine Menge, so schreiben wir  $L \subseteq_e M$ , um auszudrücken, dass  $L$  eine *endliche* Teilmenge von  $M$  ist.

Folie 304

## Sequenzen

### Definition 4.8.

(a) Eine *Sequenz* ist ein Ausdruck der Form

$$\Gamma \vdash \psi$$

wobei  $\psi \in \text{FO}[\sigma]$  und  $\Gamma \subseteq_e \text{FO}[\sigma]$  (d.h.,  $\Gamma$  ist eine *endliche* Menge von  $\text{FO}[\sigma]$ -Formeln).

Wir bezeichnen  $\Gamma$  als das *Antezedens* und  $\psi$  als das *Sukzedens* der Sequenz  $\Gamma \vdash \psi$ .

(b) Wir schreiben  $M_S$  um die Menge aller Sequenzen zu bezeichnen, d.h.:

$$M_S := \{ \Gamma \vdash \psi : \Gamma \subseteq_e \text{FO}[\sigma], \psi \in \text{FO}[\sigma] \}.$$

Folie 305

## Korrektheit einer Sequenz

**Definition 4.9.** Eine Sequenz  $\Gamma \vdash \psi$  heißt *korrekt*, falls gilt:  $\Gamma \models \psi$ .

*Zur Erinnerung:*  $\Gamma \models \psi$  bedeutet:

Für jede  $\sigma$ -Interpretation  $\mathcal{I}$  gilt: Falls  $\mathcal{I} \models \Gamma$ , so auch  $\mathcal{I} \models \psi$ .

*Beispiel:*

Welche der folgenden Sequenzen sind korrekt für alle  $\varphi, \psi \in \text{FO}[\sigma]$  und alle  $x, y \in \text{VAR}$ ; welche sind nicht korrekt?

- (1)  $\{ (\neg\varphi \vee \psi), \varphi \} \vdash \psi$
- (2)  $\emptyset \vdash (\varphi \vee \neg\varphi)$
- (3)  $\{ \exists x \forall y \varphi \} \vdash \forall y \exists x \varphi$
- (4)  $\{ \forall y \exists x x=y \} \vdash \exists x \forall y x=y$

*Antwort:*

Die ersten drei Sequenzen sind korrekt; die vierte ist nicht korrekt.

Folie 306

## Ziel

Wir wollen im Folgenden einen Kalkül  $\mathfrak{K}$  über  $M_S$  angeben, so dass gilt:

- (1)  $\mathfrak{K}$  ist *korrekt*, d.h. jede in  $\mathfrak{K}$  ableitbare Sequenz ist korrekt.
- (2)  $\mathfrak{K}$  ist *vollständig*, d.h. jede korrekte Sequenz ist in  $\mathfrak{K}$  ableitbar.
- (3)  $\mathfrak{K}$  ist *effektiv*, d.h. es gibt einen Algorithmus, der nach und nach genau die aus  $\mathfrak{K}$  ableitbaren Sequenzen aufzählt.

Dies liefert dann insbesondere einen Algorithmus, der nach und nach alle allgemeingültigen FO[ $\sigma$ ]-Formeln aufzählt: Dazu lasse den gemäß (3) existierenden Algorithmus laufen, und immer wenn dieser eine Sequenz der Form  $\Gamma \vdash \psi$  mit  $\Gamma = \emptyset$  ausgeben will, gib  $\psi$  aus.

Wegen (1) ist die Sequenz dann korrekt, d.h. es gilt  $\emptyset \models \psi$ , und daher ist  $\psi$  allgemeingültig.

Wegen (2) werden tatsächlich alle allgemeingültigen FO[ $\sigma$ ]-Formeln aufgezählt.

**Bemerkung.** Einen Kalkül  $\mathfrak{K}$  über  $M_S$  zu finden, der die Bedingungen (1) und (2) erfüllt, ist nicht schwer. Wir könnten dafür z.B. einfach den Kalkül nehmen, der aus allen Axiomen der Form

$$\overline{\Gamma \vdash \psi}$$

besteht, für die gilt:  $\Gamma \subseteq_e \text{FO}[\sigma]$ ,  $\psi \in \text{FO}[\sigma]$  und  $\Gamma \models \psi$ .

Dieser Kalkül ist offensichtlich korrekt und vollständig, d.h. er erfüllt die Bedingungen (1) und (2).

Die Bedingung (3) ist hier allerdings problematisch. Wir müssten dazu einen Algorithmus haben, der bei Eingabe einer beliebigen endlichen Menge  $\Gamma \subseteq_e \text{FO}[\sigma]$  und einer beliebigen  $\text{FO}[\sigma]$ -Formel  $\psi$  entscheidet, ob die Sequenz  $\Gamma \vdash \psi$  korrekt ist, d.h. ob gilt:  $\Gamma \models \psi$ .

Tatsächlich ist dieses Problem unentscheidbar, da (wie wir am Ende des Kapitels sehen werden) sogar bereits das

*Allgemeingültigkeitsproblem*

*Eingabe:* eine beliebige Formel  $\varphi$  der Logik erster Stufe

*Frage:* Ist  $\varphi$  allgemeingültig?

unentscheidbar ist.

Folie 307

## Notationen für Sequenzen

Wir schreiben kurz

- $\Gamma, \varphi \vdash \psi$ , um die Sequenz  $\Gamma \cup \{\varphi\} \vdash \psi$  zu bezeichnen.
- $\varphi_1, \dots, \varphi_n \vdash \psi$ , um die Sequenz  $\{\varphi_1, \dots, \varphi_n\} \vdash \psi$  zu bezeichnen.
- $\vdash \psi$ , um die Sequenz  $\emptyset \vdash \psi$  zu bezeichnen.

Folie 308

## Sequenzenregeln

Eine *Sequenzenregel* ist eine Ableitungsregel über  $M_S$ .

Sequenzenregeln der Form

$$\frac{a_1 \cdots a_n}{b}$$

schreiben wir meistens zeilenweise, als

$$\frac{\begin{array}{c} a_1 \\ \vdots \\ a_n \end{array}}{b}$$

wobei jedes  $a_i$  eine Sequenz der Form  $\Gamma_i \vdash \psi_i$  ist, und  $b$  eine Sequenz der Form  $\Delta \vdash \varphi$  ist.

Folie 309



**Definition 4.10.** Eine *Sequenzenregel*

$$\frac{\begin{array}{c} \Gamma_1 \vdash \psi_1 \\ \vdots \\ \Gamma_n \vdash \psi_n \end{array}}{\Delta \vdash \varphi}$$

heißt *korrekt*, wenn Folgendes gilt: Sind die Sequenzen  $\Gamma_i \vdash \psi_i$  für alle  $i \in \{1, \dots, n\}$  korrekt, so ist auch die Sequenz  $\Delta \vdash \varphi$  korrekt.

Aus dem Induktionsprinzip für Kalküle (Lemma 4.7) folgt direkt:

**Lemma 4.11.**

*Ein Kalkül  $\mathfrak{K}$  über  $M_S$  ist korrekt, falls jede Sequenzenregel in  $\mathfrak{K}$  korrekt ist.*

Wir werden nun eine Reihe von korrekten Sequenzenregeln zusammentragen, die alle zusammen dann den von uns gesuchten korrekten, vollständigen und effektiven Kalkül über  $M_S$  bilden werden.

Folie 310

**Grundregeln:**

Für alle  $\Gamma, \Gamma' \subseteq_e \text{FO}[\sigma]$  und alle  $\varphi \in \text{FO}[\sigma]$  betrachten wir die folgenden Sequenzenregeln:

- *Voraussetzungsregel (V):*

$$\frac{}{\Gamma, \varphi \vdash \varphi}$$

- *Erweiterungsregel (E):*

$$\frac{\Gamma \vdash \varphi}{\Gamma' \vdash \varphi} \quad \text{falls } \Gamma \subseteq \Gamma'$$

**Lemma 4.12.** *Jede der Grundregeln (V) bzw. (E) ist korrekt.*

*Beweis.* Die Voraussetzungsregel

$$(V): \quad \frac{}{\Gamma, \varphi \vdash \varphi}$$

ist korrekt, denn offensichtlich gilt:  $\Gamma \cup \{\varphi\} \models \varphi$ .

Die Erweiterungsregel

$$(E): \quad \frac{\Gamma \vdash \varphi}{\Gamma' \vdash \varphi} \quad \text{falls } \Gamma \subseteq \Gamma'$$

ist korrekt, denn:

Sei  $\Gamma \vdash \varphi$  korrekt. Dann gilt:  $\Gamma \models \varphi$ . Für  $\Gamma' \supseteq \Gamma$  gilt dann offensichtlich auch:  $\Gamma' \models \varphi$ . □

Folie 311

### Ausagenlogische Regeln:

Für alle  $\Gamma \subseteq_e \text{FO}[\sigma]$  und alle  $\varphi, \psi, \chi \in \text{FO}[\sigma]$  betrachten wir die folgenden Sequenzenregeln:

- *Fallunterscheidungsregel* (FU):

$$\frac{\Gamma, \psi \vdash \varphi \quad \Gamma, \neg\psi \vdash \varphi}{\Gamma \vdash \varphi}$$

- *Widerspruchsregel* (W):

$$\frac{\Gamma \vdash \psi \quad \Gamma \vdash \neg\psi}{\Gamma \vdash \varphi} \quad (\text{für alle } \varphi \in \text{FO}[\sigma])$$

Folie 312

- $\wedge$ -Einführung im Antezedens ( $\wedge A_1$ ), ( $\wedge A_2$ ):

$$\frac{\Gamma, \varphi \vdash \chi}{\Gamma, (\varphi \wedge \psi) \vdash \chi} \quad \frac{\Gamma, \psi \vdash \chi}{\Gamma, (\varphi \wedge \psi) \vdash \chi}$$

- $\wedge$ -Einführung im Sukzedens ( $\wedge S$ ):

$$\frac{\Gamma \vdash \varphi \quad \Gamma \vdash \psi}{\Gamma \vdash (\varphi \wedge \psi)}$$

- $\vee$ -Einführung im Antezedens ( $\vee A$ ):

$$\frac{\Gamma, \varphi \vdash \chi \quad \Gamma, \psi \vdash \chi}{\Gamma, (\varphi \vee \psi) \vdash \chi}$$

- $\vee$ -Einführung im Sukzedens ( $\vee S_1$ ), ( $\vee S_2$ ):

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash (\varphi \vee \psi)} \quad \frac{\Gamma \vdash \psi}{\Gamma \vdash (\varphi \vee \psi)}$$

Folie 313

**Lemma 4.13.** *Jede der aussagenlogischen Regeln (FU), (W), ( $\wedge A_1$ ), ( $\wedge A_2$ ), ( $\wedge S$ ), ( $\vee A$ ), ( $\vee S_1$ ), ( $\vee S_2$ ) ist korrekt.*

*Beweis.* • Die Fallunterscheidungsregel

$$(FU): \quad \frac{\Gamma, \psi \vdash \varphi \quad \Gamma, \neg\psi \vdash \varphi}{\Gamma \vdash \varphi}$$

ist korrekt, denn: Seien die beiden Sequenzen  $\Gamma, \psi \vdash \varphi$  und  $\Gamma, \neg\psi \vdash \varphi$  korrekt. Dann gilt für jede  $\sigma$ -Interpretation  $\mathcal{I}$  mit  $\mathcal{I} \models \Gamma \cup \{\psi\}$  oder  $\mathcal{I} \models \Gamma \cup \{\neg\psi\}$ , dass  $\mathcal{I} \models \varphi$ .

Wir müssen zeigen, dass die Sequenz  $\Gamma \vdash \varphi$  korrekt ist.

Sei dazu  $\mathcal{I}$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \Gamma$ .

Klar: Entweder gilt  $\mathcal{I} \models \psi$ , oder es gilt  $\mathcal{I} \models \neg\psi$ .

Im ersten Fall gilt:  $\mathcal{I} \models \Gamma \cup \{\psi\}$ , und daher folgt aus der Korrektheit der Sequenz  $\Gamma, \psi \vdash \varphi$ , dass  $\mathcal{I} \models \varphi$ .

Im zweiten Fall gilt:  $\mathcal{I} \models \Gamma \cup \{\neg\psi\}$ , und daher folgt aus der Korrektheit der Sequenz  $\Gamma, \neg\psi \vdash \varphi$ , dass  $\mathcal{I} \models \varphi$ .

Somit gilt in jedem Fall, dass  $\mathcal{I} \models \varphi$ .

Also gilt:  $\Gamma \models \varphi$ , und daher ist die Sequenz  $\Gamma \vdash \varphi$  korrekt.

- Die Widerspruchsregel

$$(W): \frac{\Gamma \vdash \psi \quad \Gamma \vdash \neg\psi}{\Gamma \vdash \varphi} \quad (\text{für alle } \varphi \in \text{FO}[\sigma])$$

ist korrekt, denn: Seien die beiden Sequenzen  $\Gamma \vdash \psi$  und  $\Gamma \vdash \neg\psi$  korrekt. Dann gilt für jede  $\sigma$ -Interpretation  $\mathcal{I}$  mit  $\mathcal{I} \models \Gamma$ , dass  $\mathcal{I} \models \psi$  und  $\mathcal{I} \models \neg\psi$ , d.h.:  $\mathcal{I} \models (\psi \wedge \neg\psi)$ . Ein solches  $\mathcal{I}$  gibt es nicht. Somit ist  $\Gamma$  unerfüllbar. Daher gilt für *jede*  $\text{FO}[\sigma]$ -Formel  $\varphi$ , dass  $\Gamma \models \varphi$ , und daher ist die Sequenz  $\Gamma \vdash \varphi$  korrekt.

- Die Regel zur  $\wedge$ -Einführung im Antezedens

$$(\wedge A_1): \frac{\Gamma, \varphi \quad \vdash \chi}{\Gamma, (\varphi \wedge \psi) \vdash \chi}$$

ist korrekt, denn: Sei die Sequenz  $\Gamma, \varphi \vdash \chi$  korrekt.

Wir müssen zeigen, dass auch die Sequenz  $\Gamma, (\varphi \wedge \psi) \vdash \chi$  korrekt ist.

Sei dazu  $\mathcal{I}$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \Gamma \cup \{(\varphi \wedge \psi)\}$ .

Insbesondere gilt dann:  $\mathcal{I} \models \Gamma$  und  $\mathcal{I} \models \varphi$ , d.h. es gilt:

$\mathcal{I} \models \Gamma \cup \{\varphi\}$ . Aus der Korrektheit der Sequenz  $\Gamma, \varphi \vdash \chi$  folgt, dass  $\mathcal{I} \models \chi$ .

Somit gilt:  $\Gamma \cup \{(\varphi \wedge \psi)\} \models \chi$ , und daher ist die Sequenz  $\Gamma, (\varphi \wedge \psi) \vdash \chi$  korrekt.

- Die Korrektheit der restlichen Regeln  $(\wedge A_2)$ ,  $(\wedge S)$ ,  $(\vee A)$ ,  $(\vee S_1)$ ,  $(\vee S_2)$  kann auf ähnliche Art gezeigt werden. Details: Übung. □

## Substitutionen

Um weitere wichtige Sequenzenregeln einführen zu können, benötigen wir eine Möglichkeit, für eine Variable  $x \in \text{VAR}$  und einen  $\sigma$ -Term  $t \in \text{T}_\sigma$  eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  so zu einer  $\text{FO}[\sigma]$ -Formel  $\varphi_x^t$  abzuändern, dass gilt:

*Die Formel  $\varphi_x^t$  sagt über den Term  $t$  dasselbe aus, wie die Formel  $\varphi$  über die Variable  $x$ .*

Präzise: Es soll für jede  $\sigma$ -Interpretation  $\mathcal{I}$  gelten:

$$\mathcal{I} \models \varphi_x^t \iff \mathcal{I}_x^t \models \varphi. \quad (4.1)$$

Dabei ist die  $\sigma$ -Interpretation  $\mathcal{I}_x^t$  für  $\mathcal{I} = (\mathcal{A}, \beta)$  wie folgt definiert:  
 $\mathcal{I}_x^t := (\mathcal{A}, \beta_x^a)$ , für  $a := \llbracket t \rrbracket^{\mathcal{I}}$ .

Außerdem soll gelten:

$$\varphi_x^x = \varphi. \quad (4.2)$$

Folie 315

Um zu gewährleisten, dass (4.1) und (4.2) gilt, wählen wir zu gegebenem  $\varphi$ ,  $t$  und  $x$  die Formel  $\varphi_x^t$  wie folgt:

- Falls  $t = x$ , so setze  $\varphi_x^t := \varphi$ . Andernfalls gehe wie folgt vor:
- Sei  $y_1, \dots, y_\ell$  eine Liste aller Variablen aus  $\text{var}(t) \cup \{x\}$ , die gebundene Vorkommen in  $\varphi$  besitzen.
- Sei  $z_1, \dots, z_\ell$  eine Liste von Variablen  $\neq x$ , die *nicht* in  $\varphi$  oder  $t$  vorkommen.
- Sei  $\varphi'$  die Formel, die aus  $\varphi$  entsteht, indem für jedes  $i \in \{1, \dots, \ell\}$  jedes *gebundene* Vorkommen der Variablen  $y_i$  ersetzt wird durch die Variable  $z_i$ .
- Sei  $\varphi_x^t$  die Formel, die aus  $\varphi'$  entsteht, indem jedes Vorkommen der Variablen  $x$  durch den Term  $t$  ersetzt wird.

Man kann zeigen:

**Lemma 4.14** (Substitutionslemma). *Für jede FO[ $\sigma$ ]-Formel  $\varphi$ , jeden  $\sigma$ -Term  $t$ , jede Variable  $x \in \text{VAR}$  und jede  $\sigma$ -Interpretation  $\mathcal{I}$  gilt:*

$$\mathcal{I} \models \varphi_x^t \iff \mathcal{I}_x^t \models \varphi.$$

*Beweis.* Übung. □

Wir können nun weitere wichtige Sequenzenregeln formulieren:

Folie 316

### Quantorenregeln:

Für alle  $\Gamma \subseteq_e \text{FO}[\sigma]$ , alle  $\varphi, \psi \in \text{FO}[\sigma]$ , alle  $x, y \in \text{VAR}$  und alle  $t \in \text{T}_\sigma$  betrachten wir die folgenden Sequenzenregeln:

- $\forall$ -Einführung im Antezedens ( $\forall A$ ):

$$\frac{\Gamma, \varphi_x^t \vdash \psi}{\Gamma, \forall x \varphi \vdash \psi}$$

- $\forall$ -Einführung im Sukzedens ( $\forall S$ ):

$$\frac{\Gamma \vdash \varphi_y^y}{\Gamma \vdash \forall x \varphi} \quad \text{falls } y \notin \text{frei}(\Gamma, \forall x \varphi)$$

- $\exists$ -Einführung im Antezedens ( $\exists A$ ):

$$\frac{\Gamma, \varphi_x^y \vdash \psi}{\Gamma, \exists x \varphi \vdash \psi} \quad \text{falls } y \notin \text{frei}(\Gamma, \exists x \varphi, \psi)$$

- $\exists$ -Einführung im Sukzedens ( $\exists S$ ):

$$\frac{\Gamma \vdash \varphi_x^t}{\Gamma \vdash \exists x \varphi}$$

Folie 317

#### Lemma 4.15.

Jede der Quantorenregeln ( $\forall A$ ), ( $\forall S$ ), ( $\exists A$ ), ( $\exists S$ ) ist korrekt.

*Beweis.* • Die Regel zur  $\forall$ -Einführung im Antezedens

$$(\forall A): \quad \frac{\Gamma, \varphi_x^t \vdash \psi}{\Gamma, \forall x \varphi \vdash \psi}$$

ist korrekt, denn: Sei die Sequenz  $\Gamma, \varphi_x^t \vdash \psi$  korrekt.

Wir müssen zeigen, dass die Sequenz  $\Gamma, \forall x \varphi \vdash \psi$  korrekt ist.

Sei dazu  $\mathcal{I}$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \Gamma \cup \{\forall x \varphi\}$ . Insbesondere gilt dann:  $\mathcal{I} \models \Gamma$ , und  $\mathcal{I}_x^a \models \varphi$  für  $a := \llbracket t \rrbracket^{\mathcal{I}}$ .

Somit gilt:  $\mathcal{I}_x^t \models \varphi$ .

Das Substitutionslemma (Lemma 4.14) liefert:  $\mathcal{I} \models \varphi_x^t$ .

Also gilt:  $\mathcal{I} \models \Gamma$  und  $\mathcal{I} \models \varphi_x^t$ .

Die Korrektheit der Sequenz  $\Gamma, \varphi_x^t \vdash \psi$  liefert:  $\mathcal{I} \models \psi$ .

Somit ist die Sequenz  $\Gamma, \forall x\varphi \vdash \psi$  korrekt.

- Die Regel zur  $\forall$ -Einführung im Sukzedens

$$(\forall S): \quad \frac{\Gamma \vdash \varphi_x^y}{\Gamma \vdash \forall x\varphi} \quad \text{falls } y \notin \text{frei}(\Gamma, \forall x\varphi)$$

ist korrekt, denn:

Sei  $y \notin \text{frei}(\Gamma, \forall x\varphi)$ , und sei die Sequenz  $\Gamma \vdash \varphi_x^y$  korrekt.

Wir müssen zeigen, dass die Sequenz  $\Gamma \vdash \forall x\varphi$  korrekt ist.

Sei dazu  $\mathcal{I} = (\mathcal{A}, \beta)$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \Gamma$ .

Wegen  $y \notin \text{frei}(\Gamma)$  gilt laut Koinzidenzlemma für alle  $a \in A$ , dass  $\mathcal{I}_y^a \models \Gamma$ . Die Korrektheit der Sequenz  $\Gamma \vdash \varphi_x^y$  liefert, dass  $\mathcal{I}_y^a \models \varphi_x^y$ .

Dies gilt für alle  $a \in A$ . Somit gilt:  $\mathcal{I} \models \forall y \varphi_x^y$ .

Wegen  $y \notin \text{frei}(\forall x\varphi)$  gilt für jede  $\sigma$ -Interpretation  $\mathcal{J}$ :

$$\mathcal{J} \models \forall y \varphi_x^y \quad \iff \quad \mathcal{J} \models \forall x \varphi.$$

Aus  $\mathcal{I} \models \forall y \varphi_x^y$  folgt also:  $\mathcal{I} \models \forall x \varphi$ .

Somit ist die Sequenz  $\Gamma \vdash \forall x\varphi$  korrekt.

- Die Korrektheit der restlichen Regeln ( $\exists A$ ) und ( $\exists S$ ) kann auf ähnliche Art gezeigt werden. Details: Übung.

□

Folie 318

## Gleichheitsregeln:

Für alle  $\Gamma \subseteq_e \text{FO}[\sigma]$ , alle  $\varphi \in \text{FO}[\sigma]$ , alle  $x \in \text{VAR}$  und alle  $t, u \in \text{T}_\sigma$  betrachten wir die folgenden Sequenzenregeln:

- *Reflexivität der Gleichheit* (G):

$$\overline{\Gamma \vdash t=t}$$

- *Substitutionsregel* (S):

$$\frac{\Gamma \quad \vdash \varphi_x^t}{\Gamma, t=u \vdash \varphi_x^u}$$

**Lemma 4.16.** *Jede der Gleichheitsregeln (G) bzw. (S) ist korrekt.*

*Beweis.* • Die Regel zur Reflexivität der Gleichheitsregel

$$(G): \quad \frac{}{\Gamma \vdash t=t}$$

ist korrekt, denn: Die Formel  $t=t$  ist offensichtlicherweise allgemeingültig. Daher gilt für *alle* Formelmengen  $\Gamma$ , dass  $\Gamma \models t=t$ . Somit ist die Sequenz  $\Gamma \vdash t=t$  korrekt.

- Die Substitutionsregel

$$(S): \quad \frac{\Gamma \quad \vdash \varphi_x^t}{\Gamma, t=u \vdash \varphi_x^u}$$

ist korrekt, denn: Sei die Sequenz  $\Gamma \vdash \varphi_x^t$  korrekt.

Wir müssen zeigen, dass die Sequenz  $\Gamma, t=u \vdash \varphi_x^u$  korrekt ist.

Sei dazu  $\mathcal{I}$  eine beliebige  $\sigma$ -Interpretation mit  $\mathcal{I} \models \Gamma \cup \{t=u\}$ .

D.h. es gilt:  $\mathcal{I} \models \Gamma$  und  $\llbracket t \rrbracket^{\mathcal{I}} = \llbracket u \rrbracket^{\mathcal{I}}$ .

Wegen  $\mathcal{I} \models \Gamma$  folgt aus der Korrektheit der Sequenz  $\Gamma \vdash \varphi_x^t$ , dass  $\mathcal{I} \models \varphi_x^t$ .

Das Substitutionslemma liefert für  $a := \llbracket t \rrbracket^{\mathcal{I}}$ , dass  $\mathcal{I}_x^a \models \varphi$ .

Wegen  $a = \llbracket t \rrbracket^{\mathcal{I}} = \llbracket u \rrbracket^{\mathcal{I}}$  gilt auch:  $\mathcal{I}_x^a \models \varphi$ .

Das Substitutionslemma liefert:  $\mathcal{I} \models \varphi_x^u$ .

Somit ist die Sequenz  $\Gamma, t=u \vdash \varphi_x^u$  korrekt.

□



## Der Sequenzenkalkül $\mathfrak{K}_S$ für die Logik erster Stufe

### Definition 4.17.

Der *Sequenzenkalkül*  $\mathfrak{K}_S$  ist der Kalkül über der Menge  $M_S$  aller Sequenzen, der für alle  $\Gamma, \Gamma' \subseteq_e \text{FO}[\sigma]$ , alle  $\varphi, \psi, \chi \in \text{FO}[\sigma]$ , alle  $t, u \in \mathsf{T}_\sigma$  und alle  $x, y \in \text{VAR}$  aus

- den Grundregeln (V), (E),
- den aussagenlogischen Regeln  
(FU), (W), ( $\wedge A_1$ ), ( $\wedge A_2$ ), ( $\wedge S$ ), ( $\vee A$ ), ( $\vee S_1$ ), ( $\vee S_2$ ),
- den Quantorenregeln ( $\forall A$ ), ( $\forall S$ ), ( $\exists A$ ), ( $\exists S$ )
- und den Gleichheitsregeln (G), (S)

besteht.

Aus der Korrektheit der Regeln des Sequenzenkalküls (Lemmas 4.12, 4.13, 4.15, 4.16) folgt mit Lemma 4.11:

**Satz 4.18.** *Der Sequenzenkalkül  $\mathfrak{K}_S$  ist korrekt, d.h. jede in  $\mathfrak{K}_S$  ableitbare Sequenz ist korrekt.*

Folie 320

Außerdem sieht man anhand der Definition der einzelnen Regeln leicht, dass es einen Algorithmus gibt, der bei Eingabe einer Zahl  $\ell \geq 1$  und einer Folge  $(a_1, \dots, a_\ell) \in M_S^\ell$  entscheidet, ob  $(a_1, \dots, a_\ell)$  eine Ableitung in  $\mathfrak{K}_S$  ist.

Für *abzählbare* Signaturen  $\sigma$  kann man außerdem einen Algorithmus angeben, der nach und nach alle Folgen in  $\{(a_1, \dots, a_\ell) \in M_S^\ell : \ell \geq 1\}$  ausgibt.

Beides zusammen liefert für abzählbare Signaturen  $\sigma$ , dass der Sequenzenkalkül  $\mathfrak{K}_S$  *effektiv* ist.

*Details:* Übung.

Unser nächstes *Ziel* ist, zu zeigen, dass der Sequenzenkalkül  $\mathfrak{K}_S$  auch *vollständig* ist, d.h. dass es für jede *korrekte* Sequenz eine Ableitung in  $\mathfrak{K}_S$  gibt.

Dazu betrachten wir zunächst einige Beispiele für Ableitungen im Sequenzenkalkül  $\mathfrak{K}_S$ .

Folie 321

## Darstellung von Ableitungen

Am Anfang des Kapitels haben wir bereits vereinbart, dass wir ähnlich wie bei Resolutionsableitungen auch allgemein für einen Kalkül  $\mathfrak{K}$  über einer Menge  $M$  Ableitungen  $(a_1, \dots, a_\ell)$  der besseren Lesbarkeit halber oft zeilenweise schreiben, also

$$\begin{array}{l} (1) \ a_1 \\ (2) \ a_2 \\ \quad \vdots \\ (\ell) \ a_\ell \end{array}$$

und am Ende jeder Zeile eine kurze Begründung angeben.

Im Folgenden betrachten wir einige Beispiele für Ableitungen im Sequenzenkalkül  $\mathfrak{K}_S$ .

Folie 322

### Beispiele 4.19.

(a) Für jedes  $\Gamma \subseteq_e \text{FO}[\sigma]$  und jedes  $\varphi \in \text{FO}[\sigma]$  ist die Sequenz  $\Gamma \vdash (\varphi \vee \neg\varphi)$  ableitbar in  $\mathfrak{K}_S$ :

$$\begin{array}{ll} (1) & \Gamma, \varphi \vdash \varphi \quad (\text{V}) \\ (2) & \Gamma, \varphi \vdash (\varphi \vee \neg\varphi) \quad (\text{VS}_1) \text{ auf (1) angewendet} \\ (3) & \Gamma, \neg\varphi \vdash \neg\varphi \quad (\text{V}) \\ (4) & \Gamma, \neg\varphi \vdash (\varphi \vee \neg\varphi) \quad (\text{VS}_2) \text{ auf (3) angewendet} \\ (5) & \Gamma \vdash (\varphi \vee \neg\varphi) \quad (\text{FU}) \text{ auf (2), (4) angewendet.} \end{array}$$

(b) Die Sequenz  $R(f(x)), \forall x x=f(x) \vdash R(f(f(x)))$  ist ableitbar in  $\mathfrak{K}_S$ :

$$\begin{array}{ll} (1) & R(f(x)) \vdash R(f(x)) \quad (\text{V}) \\ (2) & R(f(x)), x=f(x) \vdash R(f(f(x))) \quad (\text{S}) \text{ auf (1) mit} \\ & \quad \quad \quad t:=x, u:=f(x) \\ (3) & R(f(x)), \forall x x=f(x) \vdash R(f(f(x))) \quad (\forall\text{A}) \text{ auf (2) mit} \\ & \quad \quad \quad t:=x. \end{array}$$

(c) Für alle Terme  $t, u \in \mathcal{T}_\sigma$  ist die Sequenz  $t=u \vdash u=t$  ableitbar in  $\mathfrak{K}_S$ :

- (1)  $\vdash t=t$  (G)
- (2)  $t=u \vdash u=t$  (S) auf (1) mit  $\varphi := x=t$

(d) Für jedes  $\varphi \in \text{FO}[\sigma]$  ist die Sequenz  $\exists z \forall v \varphi \vdash \forall v \exists z \varphi$  ableitbar in  $\mathfrak{K}_S$ :

- (1)  $\varphi \vdash \varphi$  (V)
- (2)  $\varphi \vdash \exists z \varphi$  ( $\exists$ S) auf (1) mit  $t := z$
- (3)  $\forall v \varphi \vdash \exists z \varphi$  ( $\forall$ A) auf (2) mit  $t := v$
- (4)  $\forall v \varphi \vdash \forall v \exists z \varphi$  ( $\forall$ S) auf (3) mit  $x := v$
- (5)  $\exists z \forall v \varphi \vdash \forall v \exists z \varphi$  ( $\exists$ A) auf (4) mit  $y := z$

Folie 323

**Beweisbarkeit:**  $\Phi \vdash_{\mathfrak{K}_S} \varphi$

**Definition 4.20.** Sei  $\Phi \subseteq \text{FO}[\sigma]$  und sei  $\varphi \in \text{FO}[\sigma]$ .

Die Formel  $\varphi$  heißt *beweisbar* aus  $\Phi$  (kurz:  $\Phi \vdash_{\mathfrak{K}_S} \varphi$ ), wenn es ein  $\Gamma \subseteq_e \Phi$  gibt, so dass die Sequenz  $\Gamma \vdash \varphi$  in  $\mathfrak{K}_S$  ableitbar ist.

Ein *Beweis* von  $\varphi$  aus  $\Phi$  ist eine Ableitung einer Sequenz  $\Gamma \vdash \varphi$  in  $\mathfrak{K}_S$ , wobei  $\Gamma \subseteq_e \Phi$  ist.

**Notation.** An Stelle von  $\emptyset \vdash_{\mathfrak{K}_S} \varphi$  schreiben wir auch kurz:  $\vdash_{\mathfrak{K}_S} \varphi$ .

Aus der Korrektheit des Sequenzenkalküls  $\mathfrak{K}_S$  (Satz 4.18) folgt:

**Korollar 4.21.**

Für jede  $\text{FO}[\sigma]$ -Formel  $\varphi$  und für jede Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  gilt:

$$\Phi \vdash_{\mathfrak{K}_S} \varphi \implies \Phi \models \varphi.$$

*Beweis.*

Es gelte  $\Phi \vdash_{\mathfrak{K}_S} \varphi$ . Somit gibt es ein  $\Gamma \subseteq_e \Phi$ , so dass die Sequenz  $\Gamma \vdash \varphi$  in  $\mathfrak{K}_S$  ableitbar ist.

Gemäß Satz 4.18 ist die Sequenz  $\Gamma \vdash \varphi$  korrekt, d.h. es gilt:  $\Gamma \models \varphi$ .

Wegen  $\Gamma \subseteq \Phi$  gilt daher auch:  $\Phi \models \varphi$ . □

Folie 324

## Widerspruchsfreiheit

In der Mathematik nennen wir eine Menge von Aussagen *widerspruchsvoll*, falls sich daraus ein Widerspruch (d.h. eine bestimmte Aussage und deren Negat) herleiten lässt.

Wenn wir unter „herleiten“ einen Beweis im Sequenzenkalkül  $\mathfrak{K}_S$  verstehen, ergibt sich folgender Begriff:

**Definition 4.22.** Sei  $\Phi \subseteq \text{FO}[\sigma]$ .

- (a)  $\Phi$  heißt *widerspruchsvoll*, falls es eine  $\text{FO}[\sigma]$ -Formel  $\varphi$  gibt, so dass  $\Phi \vdash_{\mathfrak{K}_S} \varphi$  und  $\Phi \vdash_{\mathfrak{K}_S} \neg\varphi$ .
- (b)  $\Phi$  heißt *widerspruchsfrei*, falls  $\Phi$  nicht widerspruchsvoll ist.

Aus der Korrektheit des Sequenzenkalküls folgt, dass erfüllbare Formelmengen widerspruchsfrei sind:

**Korollar 4.23.** Für alle  $\Phi \subseteq \text{FO}[\sigma]$  gilt:

$$\Phi \text{ erfüllbar} \implies \Phi \text{ widerspruchsfrei.}$$

*Beweis.*

Sei  $\Phi$  erfüllbar. Dann gibt es eine  $\sigma$ -Interpretation  $\mathcal{I}$  mit  $\mathcal{I} \models \Phi$ .

Angenommen,  $\Phi$  ist nicht widerspruchsfrei. Somit ist  $\Phi$  widerspruchsvoll, d.h. es gibt eine  $\text{FO}[\sigma]$ -Formel  $\varphi$ , so dass

$$\Phi \vdash_{\mathfrak{K}_S} \varphi \quad \text{und} \quad \Phi \vdash_{\mathfrak{K}_S} \neg\varphi.$$

Korollar 4.21 liefert:

$$\Phi \models \varphi \quad \text{und} \quad \Phi \models \neg\varphi.$$

Wegen  $\mathcal{I} \models \Phi$  gilt also:

$$\mathcal{I} \models \varphi \quad \text{und} \quad \mathcal{I} \models \neg\varphi.$$

Dies ist ein *Widerspruch!* □

## Eigenschaften widerspruchsvoller Mengen

### Lemma 4.24.

Für jede Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  sind folgende Aussagen äquivalent:

- (a)  $\Phi$  ist widerspruchsvoll.
- (b) Für jede  $\text{FO}[\sigma]$ -Formel  $\psi$  gilt:  $\Phi \vdash_{\mathfrak{K}_S} \psi$ .

Beweis von Lemma 4.24.

„(b)  $\implies$  (a)“: Trivial.

„(a)  $\implies$  (b)“:

Gemäß Voraussetzung ist  $\Phi$  widerspruchsvoll.

D.h. es gibt ein  $\varphi \in \text{FO}[\sigma]$ , so dass  $\Phi \vdash_{\mathfrak{K}_S} \varphi$  und  $\Phi \vdash_{\mathfrak{K}_S} \neg\varphi$ .

Somit gibt es  $\Gamma_1, \Gamma_2 \subseteq_e \Phi$ , so dass die Sequenzen  $\Gamma_1 \vdash \varphi$  und  $\Gamma_2 \vdash \neg\varphi$  in  $\mathfrak{K}_S$  ableitbar sind.

Dann ist für jede beliebige  $\text{FO}[\sigma]$ -Formel  $\psi$  auch Folgendes in  $\mathfrak{K}_S$  ableitbar:

- (1)  $\Gamma_1 \vdash \varphi$
- (2)  $\Gamma_2 \vdash \neg\varphi$
- (3)  $\Gamma_1 \cup \Gamma_2 \vdash \varphi$  Erweiterungsregel (E) auf (1)
- (4)  $\Gamma_1 \cup \Gamma_2 \vdash \neg\varphi$  Erweiterungsregel (E) auf (2)
- (5)  $\Gamma_1 \cup \Gamma_2 \vdash \psi$  Widerspruchsregel (W) auf (3), (4)

Somit gilt  $\Phi \vdash_{\mathfrak{K}_S} \psi$  für jedes beliebige  $\psi \in \text{FO}[\sigma]$ . □

Folie 326

## Der Vollständigkeitssatz

**Satz 4.25.** Für alle Signaturen  $\sigma$ , alle Formelmengen  $\Phi \subseteq \text{FO}[\sigma]$  und alle Formeln  $\varphi \in \text{FO}[\sigma]$  gilt:

- (1)  $\Phi \vdash_{\mathfrak{K}_S} \varphi \iff \Phi \models \varphi$ .
- (2)  $\Phi$  ist widerspruchsfrei  $\iff \Phi$  ist erfüllbar.

Die Richtung „ $\implies$ “ von (1) und die Richtung „ $\impliedby$ “ von (2) haben wir bereits in Korollar 4.21 und Korollar 4.23 bewiesen.

Die Richtung „ $\implies$ “ von (2) wird von dem folgenden, schwer zu beweisenden *Erfüllbarkeitslemma* bereitgestellt:

**Lemma 4.26** (Erfüllbarkeitslemma).  
*Jede widerspruchsfreie Menge  $\Phi \subseteq \text{FO}[\sigma]$  ist erfüllbar.*

Folie 327

**Beweis des Vollständigkeitssatzes unter Verwendung des Erfüllbarkeitslemmas:**

Unter Verwendung des Erfüllbarkeitslemmas (Lemma 4.26) erhalten wir zusammen mit Korollar 4.23, dass Teil (2) des Vollständigkeitssatzes korrekt ist. D.h. für jede Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  gilt:

$$(2) \quad \Phi \text{ ist widerspruchsfrei} \iff \Phi \text{ ist erfüllbar.}$$

Die Richtung „ $\implies$ “ von (1) haben wir bereits in Korollar 4.21 gezeigt.

Die Richtung „ $\impliedby$ “ von Teil (1) des Vollständigkeitssatzes lässt sich wie folgt beweisen:

Es seien  $\Phi \subseteq \text{FO}[\sigma]$  und  $\varphi \in \text{FO}[\sigma]$ , so dass gilt:  $\Phi \models \varphi$ .

Wir wollen zeigen, dass gilt:  $\Phi \vdash_{\mathcal{R}_S} \varphi$ .

*Fall 1:*  $\Phi \cup \{\neg\varphi\}$  ist widerspruchsfrei.

Gemäß Erfüllbarkeitslemma ist  $\Phi \cup \{\neg\varphi\}$  erfüllbar. D.h. es gibt eine  $\sigma$ -Interpretation  $\mathcal{I}$ , so dass  $\mathcal{I} \models \Phi \cup \{\neg\varphi\}$ .

Somit gilt:  $\mathcal{I} \models \Phi$  und  $\mathcal{I} \not\models \varphi$ .

Aber gemäß Voraussetzung gilt:  $\Phi \models \varphi$ . Dies ist ein *Widerspruch!*

Somit kann der Fall, dass  $\Phi \cup \{\neg\varphi\}$  widerspruchsfrei ist, nicht eintreten.

*Fall 2:*  $\Phi \cup \{\neg\varphi\}$  ist *nicht* widerspruchsfrei.

Somit ist  $\Phi \cup \{\neg\varphi\}$  widerspruchsvoll.

Gemäß Lemma 4.24 gilt dann für *jede*  $\text{FO}[\sigma]$ -Formel  $\psi$ , dass

$$\Phi \cup \{\neg\varphi\} \vdash_{\mathcal{R}_S} \psi.$$

Insbesondere gilt also für die Formel  $\psi := \varphi$ , dass

$$\Phi \cup \{\neg\varphi\} \vdash_{\mathcal{R}_S} \varphi.$$

Andererseits erhält man aus der Voraussetzungsregel (V), dass

$$\Phi \cup \{\varphi\} \vdash_{\mathcal{R}_S} \varphi.$$

Die Fallunterscheidungsregel (FU) liefert:

$$\Phi \vdash_{\mathcal{R}_S} \varphi.$$

Dies beendet den Beweis des Vollständigkeitssatzes. □

Folie 328

### Zum Beweis des Erfüllbarkeitslemmas:

*Zur Erinnerung:* Das Erfüllbarkeitslemma besagt:

Jede widerspruchsfreie Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  ist erfüllbar.

#### Beweisidee:

Konstruiere eine  $\sigma$ -Interpretation  $\mathcal{I}_\Phi = (\mathcal{A}, \beta)$ , so dass gilt:

- Das Universum  $A$  von  $\mathcal{A}$  ist die Menge  $\text{T}_\sigma$  aller  $\sigma$ -Terme.
- Für jeden  $\sigma$ -Term  $t$  gilt:  $\llbracket t \rrbracket^{\mathcal{I}_\Phi} = t$ .
- Für jedes Relationssymbol  $R \in \sigma$ , für  $k := \text{ar}(R)$ , und für alle  $\sigma$ -Terme  $t_1, \dots, t_k$  gilt:

$$(t_1, \dots, t_k) \in R^{\mathcal{A}} \iff \Phi \vdash_{\mathfrak{R}_S} R(t_1, \dots, t_k)$$

Diese Interpretation  $\mathcal{I}_\Phi$  wird *Termininterpretation von  $\Phi$*  genannt.

Gemäß Definition erfüllt  $\mathcal{I}_\Phi$  alle atomaren Formeln der Form  $R(t_1, \dots, t_k)$  in  $\Phi$ .

Im Allgemeinen gilt jedoch noch nicht  $\mathcal{I}_\Phi \models \Phi$  (betrachte dazu beispielsweise die Formelmenge  $\Phi := \{v_0 = v_1\}$ , die offensichtlich erfüllbar ist, für die aber gilt:  $\mathcal{I}_\Phi \not\models \Phi$ ).

Aber nach einigen anspruchsvollen Modifikationen von  $\mathcal{I}_\Phi$  erhält man eine Interpretation  $\mathcal{I}'_\Phi$  mit  $\mathcal{I}'_\Phi \models \Phi$ .

Details finden sich im Buch „Einführung in die mathematische Logik“ von Ebbinghaus, Flum und Thomas [EFT07].

## 4.3 Der Endlichkeitssatz

Folie 329

### Zur Erinnerung:

Wir haben bereits den *Endlichkeitssatz der Aussagenlogik* kennen gelernt, der besagt, dass Folgendes für jede Menge  $\Phi \subseteq \text{AL}$  und jede Formel  $\psi \in \text{AL}$  gilt:

- (1)  $\Phi$  ist erfüllbar  $\iff$  Jede endliche Teilmenge von  $\Phi$  ist erfüllbar.
- (2)  $\Phi \models \psi$   $\iff$  Es gibt eine endliche Teilmenge  $\Gamma$  von  $\Phi$ , so dass  $\Gamma \models \psi$ .

Der Endlichkeitssatz gilt auch für die Logik erster Stufe, d.h. die Aussagen (1) und (2) gelten auch für alle Mengen  $\Phi \subseteq \text{FO}[\sigma]$  und alle  $\psi \in \text{FO}[\sigma]$ .

Zum Beweis der Endlichkeitssatzes der Logik erster Stufe nutzen wir den Vollständigkeitsatz sowie das folgende Lemma.

Folie 330

### Das syntaktische Endlichkeitslemma

**Lemma 4.27.** *Für jede Signatur  $\sigma$  und jede Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  gilt:*

$$\Phi \text{ ist widerspruchsfrei} \iff \text{Jede endliche Teilmenge von } \Phi \text{ ist widerspruchsfrei.}$$

*Beweis.*

Sei  $\sigma$  eine Signatur und sei  $\Phi \subseteq \text{FO}[\sigma]$ . Um das Lemma zu beweisen, genügt es offensichtlich, zu zeigen, dass Folgendes gilt:

$$\Phi \text{ ist widerspruchsvoll} \iff \text{Es gibt eine endliche Teilmenge von } \Phi, \text{ die widerspruchsvoll ist.}$$

Diese Aussage folgt direkt aus der Definition des Begriffs „widerspruchsvoll“, denn:

$$\begin{aligned} & \Phi \text{ ist widerspruchsvoll} \\ \stackrel{\text{Definition 4.22}}{\iff} & \text{es gibt ein } \varphi \in \text{FO}[\sigma], \text{ so dass } \Phi \vdash_{\mathfrak{K}_S} \varphi \text{ und } \Phi \vdash_{\mathfrak{K}_S} \neg\varphi \\ \stackrel{\text{Definition 4.20}}{\iff} & \text{es gibt ein } \varphi \in \text{FO}[\sigma] \text{ und Mengen } \Gamma_1, \Gamma_2 \subseteq_e \Phi, \text{ so} \\ & \text{dass die Sequenzen } \Gamma_1 \vdash \varphi \text{ und } \Gamma_2 \vdash \neg\varphi \text{ in } \mathfrak{K}_S \\ & \text{ableitbar sind} \\ \stackrel{\text{Erw.regel (E)}}{\iff} & \text{es gibt ein } \varphi \in \text{FO}[\sigma] \text{ und ein } \Gamma \subseteq_e \Phi, \text{ so dass die} \\ & \text{Sequenzen } \Gamma \vdash \varphi \text{ und } \Gamma \vdash \neg\varphi \text{ in } \mathfrak{K}_S \text{ ableitbar sind} \\ \iff & \text{es gibt ein } \varphi \in \text{FO}[\sigma] \text{ und ein } \Gamma \subseteq_e \Phi, \text{ so dass} \\ & \Gamma \vdash_{\mathfrak{K}_S} \varphi \text{ und } \Gamma \vdash_{\mathfrak{K}_S} \neg\varphi \\ \iff & \text{es gibt ein } \Gamma \subseteq_e \Phi, \text{ das widerspruchsvoll ist.} \end{aligned}$$

□



Alternativ lässt sich Lemma 4.27 auch durch Widerspruch beweisen:

„ $\implies$ “: Gemäß Voraussetzung sei  $\Phi$  widerspruchsfrei.

Sei  $\Gamma$  eine beliebige endliche Teilmenge von  $\Phi$ .

Angenommen,  $\Gamma$  ist widerspruchsvoll. Dann gibt es eine  $\text{FO}[\sigma]$ -Formel  $\varphi$ , so dass gilt:  $\Gamma \vdash_{\mathfrak{R}_S} \varphi$  und  $\Gamma \vdash_{\mathfrak{R}_S} \neg\varphi$ .

Wegen  $\Gamma \subseteq \Phi$  gilt dann auch:  $\Phi \vdash_{\mathfrak{R}_S} \varphi$  und  $\Phi \vdash_{\mathfrak{R}_S} \neg\varphi$ . Somit ist  $\Phi$  widerspruchsvoll. *Widerspruch!*

„ $\impliedby$ “: Gemäß Voraussetzung sei jede endliche Teilmenge von  $\Phi$  widerspruchsfrei. Angenommen,  $\Phi$  ist widerspruchsvoll.

Dann gibt es eine  $\text{FO}[\sigma]$ -Formel  $\varphi$ , so dass gilt:  $\Phi \vdash_{\mathfrak{R}_S} \varphi$  und  $\Phi \vdash_{\mathfrak{R}_S} \neg\varphi$ .

Gemäß Definition 4.20 gibt es dann endliche Teilmengen  $\Gamma_1$  und  $\Gamma_2$  von  $\Phi$ , so dass die Sequenzen  $\Gamma_1 \vdash \varphi$  und  $\Gamma_2 \vdash \neg\varphi$  im Sequenzenkalkül  $\mathfrak{R}_S$  ableitbar sind.

Gemäß der Erweiterungsregel (E) sind dann für  $\Gamma := \Gamma_1 \cup \Gamma_2$  auch die Sequenzen  $\Gamma \vdash \varphi$  und  $\Gamma \vdash \neg\varphi$  in  $\mathfrak{R}_S$  ableitbar.

Somit gilt:  $\Gamma \vdash_{\mathfrak{R}_S} \varphi$  und  $\Gamma \vdash_{\mathfrak{R}_S} \neg\varphi$ . Aber dies bedeutet, dass die Menge  $\Gamma$ , die ja eine endliche Teilmenge von  $\Phi$  ist, widerspruchsvoll ist.

*Widerspruch!*

□

Folie 331

## Der Endlichkeitssatz (auch bekannt als Kompaktheitssatz)

**Satz 4.28.** Für jede Signatur  $\sigma$ , jede Formelmenge  $\Phi \subseteq \text{FO}[\sigma]$  und jede Formel  $\psi \in \text{FO}[\sigma]$  gilt:

(1)  $\Phi$  ist erfüllbar  $\iff$  Jede endliche Teilmenge von  $\Phi$  ist erfüllbar.

(2)  $\Phi \models \psi \iff$  Es gibt eine endliche Teilmenge  $\Gamma$  von  $\Phi$ , so dass  $\Gamma \models \psi$ .

*Beachte:* Die Aussage des Endlichkeitssatzes ist nur für *unendliche* Formelmengen  $\Phi$  interessant (für endliche Mengen  $\Phi$  ist sie trivial).

*Beweis.* Zu (1): Es gilt:

$\Phi$ ist erfüllbar	Vollständigkeitsatz $\iff$	$\Phi$ ist widerspruchsfrei
	Lemma 4.27 $\iff$	jede endliche Teilmenge $\Gamma$ von $\Phi$ ist widerspruchsfrei
	Vollständigkeitsatz $\iff$	jede endliche Teilmenge $\Gamma$ von $\Phi$ ist erfüllbar.

Zu (2): Es gilt:

$\Phi \models \psi$	$\xLeftrightarrow{\text{Vollständigkeitsatz}}$	$\Phi \vdash_{\mathcal{K}_S} \psi$
	$\xLeftrightarrow{\text{Definition 4.20}}$	es gibt eine endliche Teilmenge $\Gamma$ von $\Phi$ , so dass $\Gamma \vdash_{\mathcal{K}_S} \psi$
	$\xLeftrightarrow{\text{Vollständigkeitsatz}}$	es gibt eine endliche Teilmenge $\Gamma$ von $\Phi$ , so dass $\Gamma \models \psi$ .

□

Folie 332

### Erststufige Axiomatisierbarkeit

#### Definition 4.29.

Eine Klasse  $\mathfrak{C}$  von  $\sigma$ -Strukturen heißt *erststufig axiomatisierbar*, falls es eine Menge  $\Phi$  von FO[ $\sigma$ ]-Sätzen gibt, so dass gilt:  $\mathfrak{C} = \text{MOD}_\sigma(\Phi)$ .

*Zur Erinnerung:*

$\text{MOD}_\sigma(\Phi)$  ist die Klasse aller  $\sigma$ -Strukturen  $\mathcal{A}$ , für die gilt:  $\mathcal{A} \models \Phi$ .

**Definition 4.30.** Die *Mächtigkeit* einer  $\sigma$ -Struktur ist die Mächtigkeit ihres Universums.

Eine  $\sigma$ -Struktur heißt endlich, unendlich, abzählbar<sup>2</sup>, bzw. überabzählbar, wenn ihr Universum die entsprechende Mächtigkeit besitzt.

#### Beispiel 4.31.

Die Klasse aller unendlichen  $\sigma$ -Strukturen ist erststufig axiomatisierbar.

*Beweis.* Für jedes  $n \in \mathbb{N}$  mit  $n \geq 1$  betrachte die FO[ $\sigma$ ]-Formel

$$\varphi_n := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leq i < j \leq n} \neg x_i = x_j.$$

Offensichtlicherweise gilt für jedes  $n \geq 1$  und für jede  $\sigma$ -Struktur  $\mathcal{A}$ :

$$\mathcal{A} \models \varphi_n \iff |A| \geq n.$$

Somit gilt für  $\Phi := \{\varphi_n : n \in \mathbb{N}, n \geq 1\}$  und für jede  $\sigma$ -Struktur  $\mathcal{A}$ :

$$\mathcal{A} \models \Phi \iff |A| = \infty.$$

Also wird die Klasse aller unendlichen Strukturen durch die Formelmengemenge  $\Phi$  erststufig axiomatisiert. □

<sup>2</sup>Wir bezeichnen eine Menge  $M$  als *abzählbar*, wenn sie entweder endlich ist oder dieselbe Mächtigkeit wie  $\mathbb{N}$  besitzt. Somit ist  $M$  genau dann abzählbar, wenn es eine injektive Abbildung von  $M$  nach  $\mathbb{N}$  gibt.

Wir können den Endlichkeitssatz anwenden, um zu zeigen, dass bestimmte Klassen von Strukturen *nicht* erststufig axiomatisierbar sind.

Im Folgenden betrachten wir dazu zwei Beispiele: die Nicht-Axiomatisierbarkeit der „Endlichkeit“ von Strukturen und die Nicht-Axiomatisierbarkeit von „Graph-Zusammenhang“.

Folie 333

### Nicht-Axiomatisierbarkeit der „Endlichkeit“ von Strukturen

**Lemma 4.32.** *Sei  $\Phi$  eine Menge von  $\text{FO}[\sigma]$ -Sätzen. Falls  $\Phi$  beliebig große endliche Modelle besitzt (d.h. für jedes  $n \in \mathbb{N}$  gibt es eine endliche  $\sigma$ -Struktur  $\mathcal{A}$  mit  $|\mathcal{A}| \geq n$  und  $\mathcal{A} \models \Phi$ ), so besitzt  $\Phi$  ein unendliches Modell.*

*Beweis.* Für  $n \geq 1$  sei  $\varphi_n$  die Formel aus dem Beweis von Beispiel 4.31, die besagt, dass das Universum mindestens  $n$  verschiedene Elemente enthält.

Sei

$$\Phi' := \Phi \cup \{\varphi_n : n \geq 1\}.$$

Dann ist jede *endliche* Teilmenge von  $\Phi'$  erfüllbar, da gemäß Voraussetzung  $\Phi$  beliebig große endliche Modelle besitzt. Gemäß Endlichkeitssatz ist auch  $\Phi'$  erfüllbar. D.h. es gibt eine  $\sigma$ -Struktur  $\mathcal{A}$  mit  $\mathcal{A} \models \Phi'$ .

Somit gilt:  $\mathcal{A} \models \Phi$  und  $\mathcal{A} \models \varphi_n$  für jedes  $n \geq 1$ . Insbesondere ist also  $|\mathcal{A}| \geq n$  für jedes  $n \in \mathbb{N}$ . Somit ist  $\mathcal{A}$  ein *unendliches* Modell von  $\Phi$ .  $\square$

### Satz 4.33.

*Die Klasse aller endlichen  $\sigma$ -Strukturen ist nicht erststufig axiomatisierbar.*

*Beweis.* Durch Widerspruch:

Angenommen,  $\Phi$  ist eine Menge von  $\text{FO}[\sigma]$ -Sätzen, die die Klasse aller endlichen  $\sigma$ -Strukturen erststufig axiomatisiert. Dann hat  $\Phi$  beliebig große endliche Modelle. Gemäß Lemma 4.32 besitzt  $\Phi$  dann auch ein unendliches Modell. *Widerspruch!*  $\square$

**Korollar 4.34.** *Es gibt keine endliche Menge von  $\text{FO}[\sigma]$ -Sätzen, die die Klasse aller unendlichen  $\sigma$ -Strukturen erststufig axiomatisiert.*

*Beweis.* Durch Widerspruch:

Angenommen,  $\Phi = \{\psi_1, \dots, \psi_m\}$  ist eine endliche Menge von  $\text{FO}[\sigma]$ -Sätzen, die die Klasse aller unendlichen  $\sigma$ -Strukturen erststufig axiomatisiert.

Dann gilt für die FO[ $\sigma$ ]-Formel

$$\varphi := \neg(\psi_1 \wedge \dots \wedge \psi_m)$$

und für jede  $\sigma$ -Struktur  $\mathcal{A}$ :

$$\mathcal{A} \models \varphi \iff \mathcal{A} \text{ ist endlich.}$$

Somit ist  $\{\varphi\}$  eine Menge von FO[ $\sigma$ ]-Sätzen, die die Klasse aller endlichen  $\sigma$ -Strukturen erststufig axiomatisiert. *Widerspruch* zu Satz 4.33.  $\square$

Folie 334

### Nicht-Axiomatisierbarkeit von „Graph-Zusammenhang“

**Satz 4.35.** *Die Klasse aller zusammenhängenden Graphen ist nicht erststufig axiomatisierbar.*

*Beweis.* Sei  $\sigma := \{E\}$  mit  $\text{ar}(E) = 2$  die Signatur für Graphen. Für jede Zahl  $n \in \mathbb{N}$  sei  $\psi_n(x, y)$  eine FO[ $\sigma$ ]-Formel, die besagt, dass es keinen Weg der Länge  $n$  von Knoten  $x$  zu Knoten  $y$  gibt. D.h. es sei

$$\psi_0(x, y) := \neg x=y$$

und, für  $n \in \mathbb{N}$  mit  $n \geq 1$ , sei

$$\psi_n(x, y) := \neg \exists z_0 \exists z_1 \dots \exists z_n \left( z_0=x \wedge z_n=y \wedge \bigwedge_{i=1}^n E(z_{i-1}, z_i) \right).$$

Offensichtlicherweise gilt für alle gerichteten Graphen  $\mathcal{A}$  und alle Knoten  $a, b \in A$ :

$$\mathcal{A} \models \psi_n[a, b] \iff \text{es gibt in } \mathcal{A} \text{ keinen Weg der Länge } n \text{ von } a \text{ nach } b.$$

Sei

$$\Psi := \{ \psi_n : n \in \mathbb{N} \}.$$

Dann gilt für jeden gerichteten Graphen  $\mathcal{A}$ , für jede Belegung  $\beta : \text{VAR} \rightarrow A$  und für die Knoten  $a := \beta(x)$  und  $b := \beta(y)$ :

$$(\mathcal{A}, \beta) \models \Psi \iff \text{es gibt in } \mathcal{A} \text{ keinen Weg von } a \text{ nach } b.$$

Angenommen,  $\Phi$  ist eine Menge von  $\text{FO}[\sigma]$ -Sätzen, die die Klasse aller zusammenhängenden Graphen erststufig axiomatisiert. D.h. für jeden ungerichteten Graphen  $\mathcal{G}$  und den zu  $\mathcal{G}$  gehörenden<sup>3</sup> gerichteten Graphen  $\mathcal{A}$  gilt:

$$\mathcal{G} \text{ ist zusammenhängend} \iff \mathcal{A} \models \Phi.$$

Gemäß Definition ist ein ungerichteter Graph  $\mathcal{G}$  genau dann zusammenhängend, wenn es für jedes Paar  $(a, b)$  von Knoten von  $\mathcal{G}$  eine Zahl  $n \in \mathbb{N}$  gibt, so dass es in  $\mathcal{G}$  einen Weg der Länge  $n$  von Knoten  $a$  zu Knoten  $b$  gibt. Daher ist

$$\Phi' := \Phi \cup \Psi$$

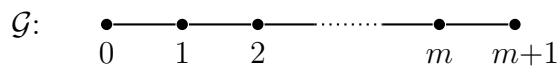
eine *unerfüllbare* Menge von  $\text{FO}[\sigma]$ -Formeln.

Im Folgenden zeigen wir, dass jede *endliche* Teilmenge  $\Gamma$  von  $\Phi'$  erfüllbar ist. Laut Endlichkeitssatz muss daher auch  $\Phi'$  erfüllbar sein. *Widerspruch!*

Sei also  $\Gamma$  eine beliebige endliche Teilmenge von  $\Phi'$ . Unser Ziel ist, zu zeigen, dass  $\Gamma$  erfüllbar ist.

Da  $\Gamma$  *endlich* ist, gibt es ein  $m \in \mathbb{N}$ , so dass für jedes  $n \in \mathbb{N}$  mit  $n > m$  gilt:  $\psi_n \notin \Gamma$  (falls  $\Gamma \cap \Psi = \emptyset$  ist, so können wir  $m := 0$  wählen; ansonsten können wir  $m := \max\{n \in \mathbb{N} : \psi_n \in \Gamma\}$  wählen). Sei  $\mathcal{G}$  ein Graph, der aus einer ungerichteten Kette von  $m+2$  Knoten besteht.

Skizze:



D.h.:  $\mathcal{G}$  ist der Graph mit Knotenmenge  $\{0, \dots, m+1\}$  und Kantenmenge  $\{\{i-1, i\} : 1 \leq i \leq m+1\}$ .

Dann gilt für die zu  $\mathcal{G}$  gehörende  $\sigma$ -Struktur  $\mathcal{A}$ :

1.  $\mathcal{A} \models \Phi$ , da  $\mathcal{G}$  zusammenhängend ist, und
2. für die Endknoten  $a := 0$  und  $b := m+1$  der Kette gilt:  
Es gibt in  $\mathcal{A}$  keinen Weg der Länge  $\leq m$  von Knoten  $a$  zu Knoten  $b$ .  
Somit gilt für jedes  $n \leq m$ , dass  $\mathcal{A} \models \psi_n[a, b]$ .

Gemäß der Wahl von  $m$  gilt daher für die Belegung  $\beta$  mit  $\beta(x) := a$  und  $\beta(y) := b$ , dass  $(\mathcal{A}, \beta) \models \Gamma$ . Somit ist  $\Gamma$  erfüllbar.  $\square$

<sup>3</sup>d.h. für  $\mathcal{G} = (V^{\mathcal{G}}, E^{\mathcal{G}})$  ist  $\mathcal{A}$  die  $\sigma$ -Struktur mit Universum  $A := V^{\mathcal{G}}$  und mit Kantenmenge  $E^{\mathcal{A}} := \{(u, v) : \{u, v\} \in E^{\mathcal{G}}\}$

## Der Satz von Löwenheim und Skolem

Unter Verwendung von Teilergebnissen, die beim (in dieser Vorlesung nicht im Detail behandelten) Beweis des Erfüllbarkeitslemmas anfallen, erhält man das folgende Resultat.

**Satz 4.36** (Der Satz von Löwenheim und Skolem).

*Sei  $\sigma$  eine abzählbare Signatur. Dann hat jede erfüllbare Formelmengemenge  $\Phi \subseteq \text{FO}[\sigma]$  ein höchstens abzählbares Modell.*

(Hier ohne Beweis)

Als direkte Folgerung aus dem Satz von Löwenheim und Skolem erhalten wir:

**Korollar 4.37.** *Sei  $\sigma$  eine abzählbare Signatur.*

*Dann ist die Klasse aller überabzählbaren  $\sigma$ -Strukturen nicht erststufig axiomatisierbar.*

*Beweis.* Angenommen,  $\Phi$  ist eine Menge von  $\text{FO}[\sigma]$ -Sätzen, die die Klasse aller überabzählbaren  $\sigma$ -Strukturen erststufig axiomatisiert.

Gemäß Satz von Löwenheim und Skolem besitzt  $\Phi$  ein höchstens abzählbares Modell. *Widerspruch!* □

## 4.4 Die Grenzen der Berechenbarkeit

Folie 336

**Zur Erinnerung:**

**Einige Begriffe zum Thema (Un)Entscheidbarkeit**

*Entscheidungsprobleme* sind Probleme, die mit „ja“ oder „nein“ beantwortet werden können. Genauer:

- Sei  $M$  eine abzählbar unendliche Menge, zum Beispiel
  - die Menge  $\Sigma^*$  aller Worte über einem endlichen Alphabet  $\Sigma$ ,  
oder
  - die Menge aller Graphen, deren Knotenmenge eine endliche Teilmenge der natürlichen Zahlen ist.
- Das *Entscheidungsproblem* für eine Menge  $L \subseteq M$  ist das folgende Berechnungsproblem:

*Das Entscheidungsproblem für  $L \subseteq M$*

*Eingabe:* Ein Element  $m \in M$ .

*Frage:* Ist  $m \in L$  ?

Folie 337

### Beispiele für Entscheidungsprobleme

- *Graphzusammenhang* ist das *Entscheidungsproblem für  $L \subseteq M$* , wobei
  - $M$  die Menge aller ungerichteten Graphen ist, deren Knotenmenge eine endliche Teilmenge von  $\mathbb{N}$  ist und
  - $L$  die Menge aller zusammenhängenden Graphen aus  $M$  ist.
- Das *Halteproblem* ist das *Entscheidungsproblem für  $L \subseteq M$* , wobei
  - $M$  die Menge aller Worte  $w\#x$  mit  $w, x \in \{0, 1\}^*$  ist und
  - $L$  die Menge aller Worte  $w\#x$  ist, so dass  $w$  eine deterministische Turingmaschine beschreibt, die bei Eingabe  $x$  nach endlich vielen Schritten anhält.

Folie 338

### Entscheidungsprobleme für die Logik erster Stufe

*Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$*

*Eingabe:* Eine  $\text{FO}[\sigma]$ -Formel  $\varphi$

*Frage:* Ist  $\varphi$  allgemeingültig?

Formal:

$M$  ist die Menge aller Worte über dem Alphabet  $A_{\text{FO}[\sigma]}$  und

$L$  ist die Menge  $\{\varphi \in \text{FO}[\sigma] : \varphi \text{ ist allgemeingültig}\}$

*Erfüllbarkeitsproblem für  $\text{FO}[\sigma]$*

*Eingabe:*  $\text{FO}[\sigma]$ -Formel  $\varphi$

*Frage:* Ist  $\varphi$  erfüllbar?

*Unerfüllbarkeitsproblem für  $\text{FO}[\sigma]$*

*Eingabe:*  $\text{FO}[\sigma]$ -Formel  $\varphi$

*Frage:* Ist  $\varphi$  unerfüllbar?

*Folgerungsproblem für FO[ $\sigma$ ]*

*Eingabe:* Zwei FO[ $\sigma$ ]-Formeln  $\varphi, \psi$

*Frage:* Gilt  $\varphi \models \psi$  ?

Folie 339

## Entscheidbarkeit und Semi-Entscheidbarkeit

**Definition 4.38.** Sei  $M$  eine abzählbar unendliche Menge.

(a) Eine Menge  $L \subseteq M$  heißt *entscheidbar*, falls es einen Algorithmus gibt, der bei Eingabe eines  $m \in M$  nach endlich vielen Schritten anhält und

- „ja“ ausgibt, falls  $m \in L$
- „nein“ ausgibt, falls  $m \notin L$ .

(b)  $L \subseteq M$  heißt *semi-entscheidbar*, falls es einen Algorithmus gibt, der bei Eingabe eines  $m \in M$

- nach endlich vielen Schritten anhält und „ja“ ausgibt, falls  $m \in L$
- nie anhält, falls  $m \notin L$ .

*Beispiele:*

- *Graphzusammenhang* ist *entscheidbar* (z.B. durch Tiefen- oder Breitensuche).
- Das *Halteproblem* ist *semi-entscheidbar* (bei Eingabe von  $w\#x$  konstruiere die von  $w$  repräsentierte deterministische Turingmaschine und lasse diese mit Eingabe  $x$  laufen).  
Ist es auch *entscheidbar*? *Nein!* — Das Halteproblem ist das Paradebeispiel eines nicht entscheidbaren Problems.

Folie 340



## Einfache Beobachtungen

- Jede entscheidbare Menge  $L \subseteq M$  ist auch semi-entscheidbar (anstatt „nein“ auszugeben und anzuhalten, gehen wir einfach in eine Endlosschleife)
- Für jede entscheidbare Menge  $L \subseteq M$  ist auch die Menge  $\bar{L} := (M \setminus L) \subseteq M$  entscheidbar (vertausche einfach die Antworten „ja“ und „nein“)
- Wenn sowohl  $L \subseteq M$  als auch  $\bar{L} := (M \setminus L) \subseteq M$  semi-entscheidbar sind, dann ist  $L \subseteq M$  sogar entscheidbar.

*Beweis:* Wir nutzen Algorithmen  $\mathbb{A}$  und  $\mathbb{B}$ , die  $L \subseteq M$  bzw.  $\bar{L} \subseteq M$  semi-entscheiden und bauen daraus einen Algorithmus  $\mathbb{C}$ , der  $L \subseteq M$  entscheidet. Bei Eingabe von  $m \in M$  geht  $\mathbb{C}$  wie folgt vor:

Für  $i = 1, 2, 3, \dots$  tue Folgendes:

Führe den  $i$ -ten Berechnungsschritt von  $\mathbb{A}$  bei Eingabe  $m$  aus.

Falls  $\mathbb{A}$  in diesem Schritt anhält, so gib „ja“ aus und halte an.

Führe den  $i$ -ten Berechnungsschritt von  $\mathbb{B}$  bei Eingabe  $m$  aus.

Falls  $\mathbb{B}$  in diesem Schritt anhält, so gib „nein“ aus und halte an.

Man sieht leicht, dass  $\mathbb{C}$  nach endlich vielen Schritten anhält und „ja“ (bzw. „nein“) ausgibt, falls  $m \in L$  (bzw.  $m \notin L$ ) ist.  $\square$

Folie 341

## Semi-Entscheidbarkeit einiger Logik-Probleme

**Satz 4.39.** *Sei  $\sigma$  eine höchstens abzählbare Signatur.*

*Jedes der folgenden Probleme ist semi-entscheidbar:*

(a) *das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$ ,*

(b) *das Unerfüllbarkeitsproblem für  $\text{FO}[\sigma]$ ,*

(c) *das Folgerungsproblem für  $\text{FO}[\sigma]$ .*

*Beweis.*

(a) Für jede FO[ $\sigma$ ]-Formel  $\varphi$  gilt gemäß dem Vollständigkeitssatz:

$$\begin{aligned} & \varphi \text{ ist allgemeingültig} \\ \iff & \emptyset \models \varphi \\ \iff & \text{die Sequenz } \emptyset \vdash \varphi \text{ ist korrekt} \\ \iff & \text{die Sequenz } \emptyset \vdash \varphi \text{ ist im Sequenzenkalkül } \mathfrak{K}_S \text{ ableitbar.} \end{aligned}$$

Da der Sequenzenkalkül  $\mathfrak{K}_S$  *effektiv* ist, gibt es einen Algorithmus  $\mathbb{S}$ , der nach und nach alle aus  $\mathfrak{K}_S$  ableitbaren Sequenzen ausgibt.

Wir nutzen diesen Algorithmus, um einen Semi-Entscheidungs-Algorithmus für das Allgemeingültigkeitsproblem für FO[ $\sigma$ ] zu erhalten: Bei Eingabe einer FO[ $\sigma$ ]-Formel  $\varphi$  starten wir  $\mathbb{S}$ . Jedesmal, wenn  $\mathbb{S}$  eine Sequenz ausgibt, überprüft  $\mathbb{A}$ , ob dies die Sequenz  $\emptyset \vdash \varphi$  ist. Falls ja, hält  $\mathbb{A}$  an und gibt „ja“ aus.

Offensichtlicherweise gilt für jede FO[ $\sigma$ ]-Formel  $\varphi$ :

Falls  $\varphi$  allgemeingültig ist, so wird  $\mathbb{A}$  bei Eingabe  $\varphi$  nach endlich vielen Schritten mit Ausgabe „ja“ anhalten (da  $\mathbb{S}$  nach endlich vielen Schritten die (korrekte) Sequenz „ $\emptyset \vdash \varphi$ “ ausgeben wird).

Falls  $\varphi$  *nicht* allgemeingültig ist, wird  $\mathbb{A}$  bei Eingabe  $\varphi$  nie anhalten (da die Sequenz „ $\emptyset \vdash \varphi$ “ nicht korrekt ist und daher nie von  $\mathbb{S}$  ausgegeben wird).

(b) Für jede FO[ $\sigma$ ]-Formel  $\psi$  gilt:

$$\varphi \text{ ist unerfüllbar} \iff \neg\varphi \text{ ist allgemeingültig.}$$

Wir können daher den Semi-Entscheidungs-Algorithmus  $\mathbb{A}$  aus (a) nutzen, um einen Semi-Entscheidungs-Algorithmus  $\mathbb{U}$  für das Unerfüllbarkeitsproblem für FO[ $\sigma$ ] zu erhalten: Bei Eingabe einer FO[ $\sigma$ ]-Formel  $\varphi$  setzen  $\psi := \neg\varphi$  und starten Algorithmus  $\mathbb{A}$  mit Eingabe  $\psi$ . Falls  $\mathbb{A}$  anhält und „ja“ ausgibt, hält auch  $\mathbb{U}$  an und gibt „ja“ aus.

Man sieht leicht, dass für jede Formel  $\varphi$  gilt: Bei Eingabe  $\varphi$  wird  $\mathbb{U}$

- nach endlich vielen Schritten anhalten und „ja“ ausgeben, falls die Formel  $\neg\varphi$  allgemeingültig, und somit  $\varphi$  unerfüllbar ist,
- nie anhalten, falls die Formel  $\neg\varphi$  *nicht* allgemeingültig, und somit  $\varphi$  erfüllbar ist.

(c) Für alle FO[ $\sigma$ ]-Formeln  $\varphi$  und  $\psi$  gilt:

$\varphi \models \psi \iff$  die Formel  $(\neg\varphi \vee \psi)$  ist allgemeingültig.

Wir können daher den Semi-Entscheidungs-Algorithmus  $\mathbb{A}$  aus (a) nutzen, um einen Semi-Entscheidungs-Algorithmus  $\mathbb{F}$  für das Folgerungsproblem zu erhalten: Bei Eingabe zweier  $\text{FO}[\sigma]$ -Formeln  $\varphi$  und  $\psi$  konstruiert  $\mathbb{F}$  die Formel  $\chi := (\neg\varphi \vee \psi)$ , startet dann Algorithmus  $\mathbb{A}$  mit Eingabe  $\chi$  und hält mit Ausgabe „ja“ an, falls  $\mathbb{A}$  mit Ausgabe „ja“ anhält.

Man sieht leicht, dass für alle Formeln  $\varphi, \psi$  gilt:

Bei Eingabe von  $\varphi$  und  $\psi$  wird  $\mathbb{F}$

- nach endlich vielen Schritten anhalten und „ja“ ausgeben, falls die Formel  $(\neg\varphi \vee \psi)$  allgemeingültig ist, und somit „ $\varphi \models \psi$ “ gilt
- nie anhalten, falls die Formel  $(\neg\varphi \vee \psi)$  *nicht* allgemeingültig ist, und somit „ $\varphi \models \psi$ “ *nicht* gilt.

□

Folie 342

## Unentscheidbarkeit einiger Logik-Probleme

Unser nächstes Ziel ist, zu zeigen, dass für bestimmte Signaturen  $\sigma$  gilt:

- Das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$ ,
- das Unerfüllbarkeitsproblem für  $\text{FO}[\sigma]$ ,
- das Erfüllbarkeitsproblem für  $\text{FO}[\sigma]$  und
- das Folgerungsproblem für  $\text{FO}[\sigma]$

ist *nicht entscheidbar*.

Wir werden dazu wie folgt vorgehen:

1. Wir nutzen das bekannte Resultat, das besagt, dass das *Postsche Korrespondenzproblem* unentscheidbar ist.
2. Wir zeigen, wie das Postsche Korrespondenzproblem unter Zuhilfenahme eines Entscheidungs-Algorithmus für das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  (für eine geeignete Signatur  $\sigma$ ) gelöst werden könnte.

Dadurch erhalten wir, dass das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  unentscheidbar ist.

3. Die Unentscheidbarkeit des Unerfüllbarkeitsproblems, des Erfüllbarkeitsproblems und des Folgerungsproblems für  $\text{FO}[\sigma]$  folgen dann leicht aus der Unentscheidbarkeit des Allgemeingültigkeitsproblems für  $\text{FO}[\sigma]$ .

Folie 343

### Das Postsche Korrespondenzproblem

*Das Postsche Korrespondenzproblem (PKP)*  
*Eingabe:* Eine Zahl  $k \geq 1$  und  $k$  Paare  $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$  mit  $x_1, y_1, \dots, x_k, y_k \in \{0, 1\}^*$ .  
*Frage:* Gibt es ein  $n \geq 1$  und Indizes  $i_1, \dots, i_n \in \{1, \dots, k\}$ , so dass gilt:  $x_{i_1}x_{i_2} \cdots x_{i_n} = y_{i_1}y_{i_2} \cdots y_{i_n}$  ?

*Beispiel:*

Das PKP mit Eingabe  $k = 3$  und

$$(x_1, y_1) = (1, 111), \quad (x_2, y_2) = (10111, 10), \quad (x_3, y_3) = (10, 0).$$

hat eine Lösung mit  $n = 4$  und  $i_1 = 2, i_2 = 1, i_3 = 1, i_4 = 3$ , denn:

$$\begin{array}{rcl} x_2 x_1 x_1 x_3 & = & 10111 \ 1 \ 1 \ 10 \\ y_2 y_1 y_1 y_3 & = & 10 \ 111 \ 111 \ 0. \end{array}$$

*Bekannt:*

- Das *PKP* ist *semi-entscheidbar*.  
 (Dies sieht man leicht.)
- Das *PKP* ist nicht *entscheidbar*.  
 (Dies wurde in der Veranstaltung „Einführung in die Theoretische Informatik“ bewiesen.)

Folie 344

## Die Unentscheidbarkeit der Logik erster Stufe

**Satz 4.40.** Sei  $\sigma := \{R, f_0, f_1, c\}$ , wobei  $c$  ein Konstantensymbol,  $R$  ein 2-stelliges Relationssymbol und  $f_0, f_1$  zwei 1-stellige Funktionssymbole sind. Das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  ist nicht entscheidbar.

*Beweis:* Auf Grund der Unentscheidbarkeit des PKP reicht es, eine Reduktion vom PKP zum Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  anzugeben. D.h. wir zeigen, dass bei Eingabe eines Tupels  $I = (k, (x_1, y_1), \dots, (x_k, y_k))$ , das eine Eingabe für's PKP repräsentiert, eine  $\text{FO}[\sigma]$ -Formel  $\varphi_I$  konstruiert werden kann, die genau dann allgemeingültig ist, wenn  $I$  eine „ja“-Instanz für's PKP ist (d.h. es gibt  $n \geq 1$  und  $i_1, \dots, i_n \in [k]$ , so dass  $x_{i_1} \cdots x_{i_n} = y_{i_1} \cdots y_{i_n}$ ).

Wenn das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  entscheidbar wäre, wäre daher auch das PKP entscheidbar.

Zur Konstruktion der Formel  $\varphi_I$  gehen wir in mehreren Schritten vor.

Folie 345

*Schritt 1:* Für jede Eingabe  $I = (k, (x_1, y_1), \dots, (x_k, y_k))$  für das PKP definiere eine  $\sigma$ -Struktur  $\mathcal{A}_I$ , so dass gilt:

$$\mathcal{A}_I \models \exists z R(z, z) \iff I \text{ ist eine „ja“-Instanz für's PKP, d.h. es gibt } n \geq 1 \text{ und } i_1, \dots, i_n \in [k], \text{ so dass } x_{i_1} \cdots x_{i_n} = y_{i_1} \cdots y_{i_n}.$$

Dazu wählen wir  $\mathcal{A}_I$  wie folgt:

- Universum  $A_I := \{0, 1\}^*$
- $c^{\mathcal{A}_I} := \varepsilon$  (leeres Wort)
- für jedes  $w \in \{0, 1\}^*$  gilt:  $f_0^{\mathcal{A}_I}(w) := w0$  und  $f_1^{\mathcal{A}_I}(w) := w1$
- $R^{\mathcal{A}_I} := \{ (x_{i_1} \cdots x_{i_n}, y_{i_1} \cdots y_{i_n}) : n \geq 1, i_1, \dots, i_n \in [k] \}$

Offensichtlicherweise gilt:

$$\mathcal{A}_I \models \exists z R(z, z) \iff I \text{ ist eine „ja“-Instanz für's PKP.}$$

Folie 346

*Schritt 2:* Konstruiere  $\text{FO}[\sigma]$ -Formeln  $\psi_I^{\text{Start}}$  und  $\psi_I^{\text{Schritt}}$ , die  $\mathcal{A}_I$  hinreichend genau beschreiben.

Die Formel  $\psi_I^{Start}$  soll besagen, dass die Relation  $R^{A_I}$  die Tupel  $(x_j, y_j)$  für alle  $j \in [k]$  enthält.

Die Formel  $\psi_I^{Schritt}$  soll besagen, dass die Relation  $R^{A_I}$  abgeschlossen ist unter Konkatination mit  $(x_j, y_j)$ ; d.h.: Ist  $(u, v) \in R^{A_I}$  und  $j \in [k]$ , so ist auch  $(ux_j, vy_j) \in R^{A_I}$ .

Um dies durch FO[ $\sigma$ ]-Formeln zu formulieren, nutzen wir folgende Schreibweisen:

Für ein Wort  $w = w_1 \cdots w_\ell \in \{0, 1\}^\ell$  und einen  $\sigma$ -Term  $t$  schreiben wir

$$f_w(t),$$

um den  $\sigma$ -Term

$$f_{w_\ell}(\cdots f_{w_2}(f_{w_1}(t)))$$

zu bezeichnen. Analog bezeichnen wir für eine  $\sigma$ -Struktur  $\mathcal{B}$  mit  $f_w^{\mathcal{B}}$  die Funktion von  $B$  nach  $B$ , so dass für jedes  $b \in B$  gilt:

$$f_w^{\mathcal{B}}(b) = f_{w_\ell}^{\mathcal{B}}(\cdots f_{w_2}^{\mathcal{B}}(f_{w_1}^{\mathcal{B}}(b))).$$

Beachte, dass dies gerade so definiert ist, dass für die Struktur  $\mathcal{A}_I$  und für alle Worte  $u \in \{0, 1\}^*$  und alle nicht-leeren  $w \in \{0, 1\}^*$  gilt:

$$f_w^{A_I}(u) = u w.$$

Unter Nutzung dieser Notationen setzen wir

$$\begin{aligned} \psi_I^{Start} &:= \bigwedge_{j=1}^k R(f_{x_j}(c), f_{y_j}(c)) \\ \psi_I^{Schritt} &:= \forall u \forall v \left( R(u, v) \rightarrow \bigwedge_{j=1}^k R(f_{x_j}(u), f_{y_j}(v)) \right) \end{aligned}$$

Beachte:  $\mathcal{A}_I \models (\psi_I^{Start} \wedge \psi_I^{Schritt})$ , da die Relation  $R^{A_I}$  alle Tupel  $(x_j, y_j)$  für  $j \in [k]$  enthält und da für alle Tupel  $(u, v) \in R^{A_I}$  gilt, dass auch  $(ux_j, vy_j) \in R^{A_I}$  ist, für jedes  $j \in [k]$ .

Folie 347

*Schritt 3:* Setze  $\varphi_I := \left( (\psi_I^{Start} \wedge \psi_I^{Schritt}) \rightarrow \exists z R(z, z) \right)$

Klar: Es gibt einen Algorithmus, der bei Eingabe von  $I$  die Formel  $\varphi_I$  konstruiert.

*Behauptung 1:*

$\varphi_I$  ist allgemeingültig  $\iff I$  ist eine „ja“-Instanz für's PKP.

*Beweis:*

„ $\implies$ “: Sei  $\varphi_I$  allgemeingültig. Dann gilt insbesondere  $\mathcal{A}_I \models \varphi_I$ . Gemäß Schritt 2 und Schritt 1 ist  $I$  dann eine „ja“-Instanz für's PKP.

„ $\impliedby$ “: Sei  $I$  eine „ja“-Instanz für's PKP. Dann gibt es ein Wort  $\hat{u} \in \{0, 1\}^*$ , so dass  $(\hat{u}, \hat{u}) \in R^{\mathcal{A}_I}$ .

Wir müssen zeigen, dass  $\varphi_I$  allgemeingültig ist. Sei dazu  $\mathcal{B}$  eine beliebige  $\sigma$ -Struktur. Zu zeigen:  $\mathcal{B} \models \varphi_I$ .

*Fall 1:*  $\mathcal{B} \not\models (\psi_I^{\text{Start}} \wedge \psi_I^{\text{Schritt}})$ .

Dann gilt gemäß Konstruktion von  $\varphi_I$ , dass  $\mathcal{B} \models \varphi_I$ .

*Fall 2:*  $\mathcal{B} \models (\psi_I^{\text{Start}} \wedge \psi_I^{\text{Schritt}})$ .

Wir müssen zeigen, dass dann auch gilt:  $\mathcal{B} \models \exists z R(z, z)$ . D.h. wir müssen ein  $\hat{b} \in B$  finden, so dass gilt:  $(\hat{b}, \hat{b}) \in R^{\mathcal{B}}$ .

Ein solches  $\hat{b} \in B$  finden wir, indem wir  $\hat{b} := h(\hat{u})$  setzen, wobei  $h : \{0, 1\}^* \rightarrow B$  wie folgt definiert ist:

$$\begin{aligned} h(\varepsilon) &:= c^{\mathcal{B}}, & \text{und für alle } u \in \{0, 1\}^* \text{ gilt:} \\ h(u0) &:= f_0^{\mathcal{B}}(h(u)), \\ h(u1) &:= f_1^{\mathcal{B}}(h(u)). \end{aligned}$$

Per Induktion nach der Länge von  $w$  sieht man leicht, dass für alle  $u \in \{0, 1\}^*$  und alle nicht-leeren  $w \in \{0, 1\}^*$  gilt:

$$h(uw) = f_w^{\mathcal{B}}(h(u)) \quad \text{und} \quad h(w) = f_w^{\mathcal{B}}(h(\varepsilon)) = f_w^{\mathcal{B}}(c^{\mathcal{B}}).$$

Wegen  $(\hat{u}, \hat{u}) \in R^{\mathcal{A}_I}$  folgt daher aus der nächsten Behauptung, dass  $(\hat{b}, \hat{b}) \in R^{\mathcal{B}}$ , und damit ist der Beweis dann beendet.

*Behauptung 2:* Für alle  $(u, v) \in R^{\mathcal{A}_I}$  gilt:  $(h(u), h(v)) \in R^{\mathcal{B}}$ .

*Beweis:* Per Induktion nach  $n$  zeigen wir, dass für alle  $n \geq 1$  und alle  $i_1, \dots, i_n \in [k]$  gilt:  $(h(x_{i_1} \cdots x_{i_n}), h(y_{i_1} \cdots y_{i_n})) \in R^{\mathcal{B}}$ .

*Induktionsanfang*  $n = 1$ : Wegen  $\mathcal{B} \models \psi_I^{\text{Start}}$  gilt insbes. für  $j := i_1$ , dass

$$\mathcal{B} \models R(f_{x_{i_1}}(c), f_{y_{i_1}}(c)).$$

Somit gilt:  $(h(x_{i_1}), h(y_{i_1})) = (f_{x_{i_1}}^{\mathcal{B}}(c^{\mathcal{B}}), f_{y_{i_1}}^{\mathcal{B}}(c^{\mathcal{B}})) \in R^{\mathcal{B}}$ . Dies beendet den Induktionsanfang.

*Induktionsschritt*  $n \rightarrow n+1$ : Gemäß Induktionsannahme gilt für  $u := x_{i_1} \cdots x_{i_n}$  und  $v := y_{i_1} \cdots y_{i_n}$ , dass  $(h(u), h(v)) \in R^{\mathcal{B}}$ . Für  $j := i_{n+1}$  müssen wir zeigen, dass auch gilt:  $(h(ux_j), h(vy_j)) \in R^{\mathcal{B}}$ . Wegen  $\mathcal{B} \models \psi_I^{\text{Schritt}}$  und  $(h(u), h(v)) \in R^{\mathcal{B}}$  gilt gemäß der Konstruktion von  $\psi_I^{\text{Schritt}}$ , dass

$$\left( h(ux_j), h(vy_j) \right) = \left( f_{x_j}^{\mathcal{B}}(h(u)), f_{y_j}^{\mathcal{B}}(h(v)) \right) \in R^{\mathcal{B}}.$$

Dies beendet den Induktionsschritt und daher auch den Beweis von Behauptung 2, den Beweis von Behauptung 1 und insgesamt den Beweis von Satz 4.40. □

Folie 348

Aus Satz 4.39, Satz 4.40 und den bekannten Zusammenhängen zwischen semi-entscheidbaren und entscheidbaren Problemen, sowie den Korrespondenzen zwischen Allgemeingültigkeit, (Un)Erfüllbarkeit und logischer Folgerung, erhält man leicht:

**Korollar 4.41.** *Sei  $\sigma$  die Signatur aus Satz 4.40. Dann gilt:*

- (a) *Das Allgemeingültigkeitsproblem für  $\text{FO}[\sigma]$  ist semi-entscheidbar aber nicht entscheidbar.*
- (b) *Das Folgerungsproblem für  $\text{FO}[\sigma]$  ist semi-entscheidbar aber nicht entscheidbar.*
- (c) *Das Unerfüllbarkeitsproblem für  $\text{FO}[\sigma]$  ist semi-entscheidbar aber nicht entscheidbar.*
- (d) *Das Erfüllbarkeitsproblem für  $\text{FO}[\sigma]$  ist nicht semi-entscheidbar.*

*Beweis:* Übung.

Folie 349

**Bemerkung 4.42.** Man kann zeigen, dass

- (1) Korollar 4.41 für jede Signatur  $\sigma$  gilt, die mindestens ein Relationssymbol der Stelligkeit  $\geq 2$  enthält
- (2) für Signaturen  $\sigma$ , die ausschließlich aus Konstantensymbolen und Relationssymbolen der Stelligkeit 1 bestehen, jedes der in Korollar 4.41 betrachteten Probleme entscheidbar ist.

(Hier ohne Beweis)



## 4.5 Der Satz von Herbrand

Folie 350

- Im letzten Abschnitt haben wir gesehen, dass es keinen Algorithmus gibt, der das Erfüllbarkeitsproblem und das Allgemeingültigkeitsproblem der Logik erster Stufe löst und stets terminiert.
- Trotzdem möchte man für verschiedene Anwendungsbereiche Verfahren haben, die das Erfüllbarkeits- oder das Allgemeingültigkeitsproblem der Logik erster Stufe „so gut wie möglich“ lösen.
- Einen Ansatz für die Entwicklung solcher, in der Praxis nutzbarer, Verfahren liefert die *Herbrand-Theorie*, die nach dem französischen Logiker Jacques Herbrand (1908–1931) benannt ist.
- Ziel dieses Abschnitts ist, den *Satz von Herbrand* vorzustellen, der das Allgemeingültigkeits- bzw. das Erfüllbarkeitsproblem der Logik erster Stufe auf das entsprechende Problem der Aussagenlogik zurückführt.

Folie 351

### Notationen

- In diesem Abschnitt bezeichnet  $\sigma$  stets eine endliche oder abzählbare Signatur, die mindestens ein Konstantensymbol enthält.
- Die Menge aller *quantorenfreien*  $\text{FO}[\sigma]$ -Formeln bezeichnen wir mit  $\text{QF}_\sigma$ .
- Ein *Grundterm* über  $\sigma$  ist ein *variablenfreier*  $\sigma$ -Term, d.h., ein  $\sigma$ -Term, der keine Variable enthält.  
Die Menge aller Grundterme über  $\sigma$  bezeichnen wir mit  $\text{GT}_\sigma$ .

*Beispiele:*

(a) Sei  $\sigma := \{c, f/1, g/2, R/2\}$ .

Grundterme über  $\sigma$  sind dann z.B.

$c, f(c), g(c, c), f(f(c)), f(g(c, c)), g(c, f(c)), g(f(c), c), \dots$

(b) Sei  $\sigma := \{c, R/2\}$ .

Dann ist  $c$  der einzige Grundterm über  $\sigma$ . D.h.

$$\text{GT}_\sigma = \{c\}.$$

Folie 352

## Herbrandstrukturen

**Definition 4.43.** Sei  $\sigma$  eine Signatur, die mindestens ein Konstantensymbol enthält.

Eine  $\sigma$ -Herbrandstruktur ist eine  $\sigma$ -Struktur  $\mathcal{A}$  mit folgenden Eigenschaften:

- Das Universum  $A$  von  $\mathcal{A}$  ist genau die Menge  $\text{GT}_\sigma$  aller Grundterme über  $\sigma$  (d.h. aller variablenfreien  $\sigma$ -Terme).
- Für jedes Konstantensymbol  $c \in \sigma$  ist  $c^{\mathcal{A}} = c$ .
- Für jedes Funktionssymbol  $f \in \sigma$ , für  $k := \text{ar}(f)$ , und für alle variablenfreien  $\sigma$ -Terme  $t_1, \dots, t_k \in A$  ist

$$f^{\mathcal{A}}(t_1, \dots, t_k) = f(t_1, \dots, t_k).$$

*Beachte:* Alle  $\sigma$ -Herbrandstrukturen haben dasselbe Universum und dieselbe Interpretation der Konstanten- und Funktionssymbole.

Lediglich die Interpretation der Relationssymbole kann in  $\sigma$ -Herbrandstrukturen frei gewählt werden.

Zur Angabe einer konkreten  $\sigma$ -Herbrandstruktur  $\mathcal{A}$  genügt es also, die Interpretation der Relationssymbole anzugeben, d.h. für jedes Relationssymbol  $R \in \sigma$  die Relation  $R^{\mathcal{A}}$  anzugeben.

Folie 353

## Beispiel

Sei  $\sigma := \{c, R/2\}$ .

*Frage:* Wie sehen  $\sigma$ -Herbrandstrukturen aus?

*Antwort:* Für jede  $\sigma$ -Herbrandstruktur  $\mathcal{A}$  gilt:

- Universum:  $A = \{c\}$
- $c^{\mathcal{A}} = c$

- $R^{\mathcal{A}} \subseteq \{c\}^2$ , d.h.

$$R^{\mathcal{A}} = \emptyset \quad \text{oder} \quad R^{\mathcal{A}} = \{ (c, c) \}.$$

Somit gibt es genau 2 verschiedene  $\sigma$ -Herbrandstrukturen.

Folie 354

**Bemerkung 4.44.** Sei  $\mathcal{A}$  eine  $\sigma$ -Herbrandstruktur.

Man sieht leicht, dass Folgendes gilt:

- Für jeden variablenfreien  $\sigma$ -Term  $t$  (d.h. für jedes  $t \in \text{GT}_{\sigma} = A$ ) gilt:

$$\llbracket t \rrbracket^{\mathcal{A}} = t.$$

- Für jede quantorenfreie FO[ $\sigma$ ]-Formel  $\psi$  gilt:  
Ist  $\text{var}(\psi) \subseteq \{x_1, \dots, x_n\}$  und sind  $t_1, \dots, t_n \in \text{GT}_{\sigma}$ , so gilt:

$$\mathcal{A} \models \psi[t_1, \dots, t_n] \quad \iff \quad \mathcal{A} \models \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n}$$

Dabei ist  $\psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n}$  die Formel, die aus  $\psi$  entsteht, indem für jedes  $i \in [n]$  jedes Vorkommen von  $x_i$  ersetzt wird durch den Grundterm  $t_i$ .

Folie 355

## Herbrand-Modelle und gleichheitsfreie Formeln in Skolemform

**Definition 4.45.**

- Ein *Herbrand-Modell* eines FO[ $\sigma$ ]-Satzes  $\varphi$  ist eine  $\sigma$ -Herbrandstruktur, die  $\varphi$  erfüllt.
- Eine FO[ $\sigma$ ]-Formel  $\varphi$  heißt *gleichheitsfrei*, falls das Symbol „ $=$ “ nicht in  $\varphi$  vorkommt.
- Eine FO[ $\sigma$ ]-Formel ist in *Skolemform* (auch: *Skolem-Normalform*), falls sie von der Form

$$\forall x_1 \dots \forall x_n \psi$$

ist, wobei gilt:  $n \geq 0$ ,  $x_1, \dots, x_n$  sind paarweise verschiedene Variablen, und  $\psi$  ist eine quantorenfreie FO[ $\sigma$ ]-Formel.

**Satz 4.46.**

Sei  $\sigma$  eine Signatur, die mindestens ein Konstantensymbol besitzt.

Für jeden gleichheitsfreien FO[ $\sigma$ ]-Satz  $\varphi$  in Skolemform gilt:

$$\varphi \text{ ist erfüllbar} \iff \varphi \text{ besitzt ein Herbrand-Modell.}$$

*Beweis.*

Die Richtung „ $\Leftarrow$ “ ist offensichtlich.

Für den Beweis der Richtung „ $\Rightarrow$ “ sei  $\mathcal{B}$  eine  $\sigma$ -Struktur mit  $\mathcal{B} \models \varphi$ . Wir definieren im Folgenden eine  $\sigma$ -Herbrandstruktur  $\mathcal{A}$  und zeigen dann, dass gilt:  $\mathcal{A} \models \varphi$ .

Wir definieren die  $\sigma$ -Herbrandstruktur  $\mathcal{A}$  wie folgt: Für jedes Relationssymbol  $R \in \sigma$ , für  $k := \text{ar}(R)$  und für alle  $t_1, \dots, t_k \in \text{GT}_\sigma = A$  setze

$$(t_1, \dots, t_k) \in R^{\mathcal{A}} \iff \mathcal{B} \models R(t_1, \dots, t_k).$$

Per Induktion über den Aufbau von Formeln erhält man leicht (Details: Übung), dass für alle  $n \in \mathbb{N}$ , für alle gleichheitsfreien quantorenfreien FO[ $\sigma$ ]-Formeln  $\psi$  mit  $\text{var}(\psi) \subseteq \{x_1, \dots, x_n\}$  und für alle  $t_1, \dots, t_n \in \text{GT}_\sigma$  gilt:

$$\mathcal{A} \models \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n} \iff \mathcal{B} \models \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n} \quad (4.3)$$

Laut Voraussetzung gilt  $\mathcal{B} \models \varphi$ , und  $\varphi$  ist von der Form  $\forall x_1 \cdots \forall x_n \psi$ , wobei  $\psi$  eine gleichheitsfreie, quantorenfreie FO[ $\sigma$ ]-Formel ist.

Wegen  $\mathcal{B} \models \forall x_1 \cdots \forall x_n \psi$  gilt insbes. für alle Grundterme  $t_1, \dots, t_n \in \text{GT}_\sigma$ , dass

$$\mathcal{B} \models \psi [ [t_1]^{\mathcal{B}}, \dots, [t_n]^{\mathcal{B}} ],$$

und somit gilt auch:

$$\mathcal{B} \models \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n}$$

für alle  $t_1, \dots, t_n \in \text{GT}_\sigma$ .

Aus (4.3) folgt, dass

$$\mathcal{A} \models \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n}$$

für alle  $t_1, \dots, t_n \in \text{GT}_\sigma = A$  gilt.

Somit gilt:  $\mathcal{A} \models \forall x_1 \cdots \forall x_n \psi$ . Also ist  $\mathcal{A}$  ein Herbrand-Modell von  $\varphi$ .  $\square$

## Die Herbrand-Expansion eines Satzes in Skolemform

**Definition 4.47.** Sei  $\varphi$  ein gleichheitsfreier FO[ $\sigma$ ]-Satz in Skolemform, d.h.  $\varphi$  ist von der Form  $\forall x_1 \cdots \forall x_n \psi$ , wobei  $\psi$  quantorenfrei und gleichheitsfrei ist.

Die *Herbrand-Expansion* von  $\varphi$  ist die Formelmenge

$$\text{HE}(\varphi) := \left\{ \psi \frac{t_1, \dots, t_n}{x_1, \dots, x_n} : t_1, \dots, t_n \in \text{GT}_\sigma \right\}$$

D.h.: Jede Formel in  $\text{HE}(\varphi)$  entsteht, indem in der quantorenfreien Formel  $\psi$  jede Variable  $x_i$  ersetzt wird durch einen Grundterm  $t_i$ .

**Beispiel 4.48.** Sei  $\sigma = \{c, f/1, g/2, R/3\}$  und sei

$$\varphi := \forall x \forall y \forall z R(x, f(y), g(z, x))$$

Dann gehören z.B. die folgenden Formeln zur Herbrand-Expansion  $\text{HE}(\varphi)$ :

- $R(c, f(c), g(c, c))$   
(dies erhält man, indem jede der Variablen  $x, y, z$  durch den Grundterm  $c$  ersetzt wird)
- $R(f(c), f(c), g(c, f(c)))$   
(dies erhält man, indem  $x$  durch den Grundterm  $f(c)$  und jede der Variablen  $y, z$  durch den Grundterm  $c$  ersetzt wird)
- $R(g(c, c), f(f(c)), g(c, g(c, c)))$   
(dies erhält man, indem Variable  $x$  durch den Grundterm  $g(c, c)$ , Variable  $y$  durch den Grundterm  $f(c)$  und Variable  $z$  durch den Grundterm  $c$  ersetzt wird)

Folie 357

## Die aussagenlogische Version der Herbrand-Expansion

Für jeden gleichheitsfreien FO[ $\sigma$ ]-Satz  $\varphi$  in Skolemform gilt:

Jede Formel  $\xi \in \text{HE}(\varphi)$  ist quantorenfrei, gleichheitsfrei und variablenfrei, und jede atomare Subformel von  $\xi$  ist von der Form  $R(t_1, \dots, t_k)$ , wobei  $R \in \sigma$ ,  $k = \text{ar}(R)$  und  $t_1, \dots, t_k \in \text{GT}_\sigma$ .

Für jede solche atomare Formel stellen wir ein *Aussagensymbol*  $X_{R(t_1, \dots, t_k)} \in \text{AS}$  bereit.

Für jedes  $\xi \in \text{HE}(\varphi)$  sei  $\text{al}(\xi)$  die *aussagenlogische* Formel, die aus  $\xi$  entsteht, indem jede atomare Subformel der Form  $R(t_1, \dots, t_k)$  ersetzt wird durch das Aussagensymbol  $X_{R(t_1, \dots, t_k)}$ .

Die *aussagenlogische Version der Herbrand-Expansion* von  $\varphi$  ist die Menge

$$\text{AHE}(\varphi) := \{ \text{al}(\xi) : \xi \in \text{HE}(\varphi) \}.$$

Folie 358

### Der Satz von Herbrand

**Satz 4.49** (Satz von Gödel-Herbrand-Skolem).

*Sei  $\sigma$  eine Signatur, die mindestens ein Konstantensymbol enthält.*

*Für jeden gleichheitsfreien FO[ $\sigma$ ]-Satz  $\varphi$  in Skolemform gilt:  $\varphi$  ist erfüllbar  $\iff$  die aussagenlogische Formelmenge  $\text{AHE}(\varphi)$  ist erfüllbar.*

*Beweis.* Sei  $\varphi$  von der Form  $\forall x_1 \dots \forall x_n \psi$ , wobei  $\psi$  quantorenfrei und gleichheitsfrei ist. Es gilt:

$$\begin{aligned} & \varphi \text{ ist erfüllbar} \\ \stackrel{\text{Satz 4.46}}{\iff} & \varphi \text{ besitzt ein Herbrand-Modell} \\ \iff & \text{es gibt eine } \sigma\text{-Herbrandstruktur } \mathcal{A} \text{ mit } \mathcal{A} \models \forall x_1 \dots \forall x_n \psi \end{aligned}$$

Für jede  $\sigma$ -Herbrandstruktur  $\mathcal{A}$  gilt:

$$\begin{aligned} & \mathcal{A} \models \forall x_1 \dots \forall x_n \psi \\ \stackrel{\mathcal{A} \models \text{GT}_\sigma}{\iff} & \text{für alle } t_1, \dots, t_n \in \text{GT}_\sigma \text{ gilt: } \mathcal{A} \models \psi_{\frac{t_1, \dots, t_n}{x_1, \dots, x_n}} \\ \stackrel{\text{Def. HE}(\varphi)}{\iff} & \mathcal{A} \models \text{HE}(\varphi) \\ \iff & \mathcal{J}_\mathcal{A} \models \text{AHE}(\varphi), \end{aligned}$$

wobei  $\mathcal{J}_\mathcal{A}$  die *aussagenlogische* Interpretation ist, so dass für jedes  $R \in \sigma$ , für  $k := \text{ar}(R)$ , für alle Grundterme  $t_1, \dots, t_k \in \text{GT}_\sigma$  und für das zugehörige Aussagensymbol  $X_{R(t_1, \dots, t_k)}$  gilt:

$$\mathcal{J}_\mathcal{A} ( X_{R(t_1, \dots, t_k)} ) := \begin{cases} 1 & \text{falls } \mathcal{A} \models R(t_1, \dots, t_k) \\ 0 & \text{sonst} \end{cases}$$

Insbesondere folgt, dass gilt:

$$\varphi \text{ erfüllbar} \implies \text{AHE}(\varphi) \text{ erfüllbar.}$$

Umgekehrt sei für jede aussagenlogische Interpretation  $\mathcal{J}$  die zu  $\mathcal{J}$  gehörende  $\sigma$ -Herbrandstruktur  $\mathcal{A}_{\mathcal{J}}$  definiert via

$$R^{\mathcal{A}_{\mathcal{J}}} := \left\{ (t_1, \dots, t_k) : t_1, \dots, t_k \in \text{GT}_{\sigma} \text{ und } \mathcal{J}(X_{R(t_1, \dots, t_k)}) = 1 \right\},$$

für jedes  $R \in \sigma$  und für  $k = \text{ar}(R)$ .

Man sieht leicht, dass für jede aussagenlogische Interpretation  $\mathcal{J}$  und jedes  $\xi \in \text{HE}(\varphi)$  gilt:

$$\mathcal{J} \models \text{al}(\xi) \iff \mathcal{A}_{\mathcal{J}} \models \xi.$$

Somit gilt auch:

$$\mathcal{J} \models \text{AHE}(\varphi) \iff \mathcal{A}_{\mathcal{J}} \models \text{HE}(\varphi) \iff \mathcal{A}_{\mathcal{J}} \models \varphi.$$

Insbesondere gilt also:

$$\text{AHE}(\varphi) \text{ erfüllbar} \implies \varphi \text{ erfüllbar}.$$

Dies beendet den Beweis von Satz 4.49. □

In Verbindung mit dem Endlichkeitssatz der Aussagenlogik erhalten wir:

**Satz 4.50** (Satz von Herbrand).

Sei  $\sigma$  eine Signatur, die mindestens ein Konstantensymbol enthält. Sei  $\psi$  eine gleichheitsfreie und quantorenfreie  $\text{FO}[\sigma]$ -Formel und sei  $\{x_1, \dots, x_n\} = \text{frei}(\psi)$ .

Dann gilt für die  $\text{FO}[\sigma]$ -Sätze  $\varphi := \forall x_1 \dots \forall x_n \psi$  und  $\varphi' := \exists x_1 \dots \exists x_n \psi$ :

(a)  $\varphi$  ist erfüllbar  $\iff$  jede endliche Teilmenge von  $\text{AHE}(\varphi)$  ist erfüllbar.

(b)  $\varphi$  ist unerfüllbar  $\iff$  es gibt eine endliche Teilmenge von  $\text{AHE}(\varphi)$ , die unerfüllbar ist.

(c)  $\varphi'$  ist allgemeingültig  $\iff$  es gibt eine Zahl  $m \in \mathbb{N}$  und Grundterme  $t_{i,1}, \dots, t_{i,n}$  für alle  $i \in [m]$ , so dass die folgende Formel allgemeingültig ist:

$$\bigvee_{i=1}^m \psi_{\substack{t_{i,1}, \dots, t_{i,n} \\ x_1, \dots, x_n}}$$

*Beweis.*

Aussage (a) folgt direkt aus dem Satz von Gödel-Herbrand-Skolem und dem Endlichkeitssatz der Aussagenlogik.

Aussage (b) folgt direkt aus (a).

Aussage (c) lässt sich aus (b) wie folgt herleiten:

Offensichtlicherweise gilt:

$$\varphi' \text{ ist allgemeingültig} \iff \neg\varphi' \text{ ist unerfüllbar.}$$

Außerdem ist

$$\neg\varphi' = \neg\exists x_1 \cdots \exists x_n \psi \equiv \forall x_1 \cdots \forall x_n \neg\psi.$$

Gemäß (b) ist  $\neg\varphi'$  genau dann unerfüllbar, wenn es eine endliche Teilmenge  $\Gamma$  von  $\text{AHE}(\forall x_1 \cdots \forall x_n \neg\psi)$  gibt, die unerfüllbar ist.

Gemäß der Definition der Herbrand-Expansion einer Formel ist jede endliche Teilmenge  $\Gamma$  von  $\text{AHE}(\forall x_1 \cdots \forall x_n \neg\psi)$  von der Form

$$\left\{ \text{al} \left( \neg\psi \frac{t_{i,1}, \dots, t_{i,n}}{x_1, \dots, x_n} \right) : i \in \{1, \dots, m\} \right\},$$

wobei  $m \in \mathbb{N}$  und  $t_{i,1}, \dots, t_{i,n} \in \text{GT}_\sigma$  für jedes  $i \in [m]$  ist.

Eine solche Formelmengung ist genau dann unerfüllbar, wenn die aussagenlogische Formel

$$\bigwedge_{i=1}^m \text{al} \left( \neg\psi \frac{t_{i,1}, \dots, t_{i,n}}{x_1, \dots, x_n} \right)$$

unerfüllbar ist.

Dies wiederum ist genau dann der Fall, wenn der quantorenfreie und gleichheitsfreie  $\text{FO}[\sigma]$ -Satz

$$\bigwedge_{i=1}^m \neg\psi \frac{t_{i,1}, \dots, t_{i,n}}{x_1, \dots, x_n}$$

unerfüllbar ist.

Und dies gilt genau dann, wenn der  $\text{FO}[\sigma]$ -Satz

$$\bigvee_{i=1}^m \psi \frac{t_{i,1}, \dots, t_{i,n}}{x_1, \dots, x_n}$$

allgemeingültig ist.

Dies beendet den Beweis von (c). □



## Anwendung des Satzes von Herbrand

Um nachzuweisen, dass ein gleichheitsfreier  $\text{FO}[\sigma]$ -Satz  $\varphi$  in Skolemform unerfüllbar ist, kann man auf Grund des Satzes von Herbrand wie folgt vorgehen:

Für  $i = 1, 2, 3, \dots$  tue Folgendes:

- (1) Sei  $\xi_i$  die  $i$ -te Formel in  $\text{AHE}(\varphi)$
- (2) Teste, ob die aussagenlogische Formel  $(\xi_1 \wedge \dots \wedge \xi_i)$  unerfüllbar ist.
- (3) Falls ja, halte an mit Ausgabe „ $\varphi$  ist unerfüllbar“

Man sieht leicht, dass dies ein Semi-Entscheidungsverfahren ist, das eine gegebene Formel  $\varphi$  auf Unerfüllbarkeit testet.

Durch die Einschränkung auf *gleichheitsfreie*  $\text{FO}[\sigma]$ -Sätze in Skolemform scheint dieses Verfahren auf den ersten Blick nur sehr eingeschränkt anwendbar zu sein.

Im Folgenden zeigen wir jedoch, dass *jede*  $\text{FO}[\sigma]$ -Formel in eine zu ihr erfüllbarkeitsäquivalente Formel der richtigen Form transformiert werden kann.

Folie 360

**Definition 4.51.** Seien  $\sigma_1, \sigma_2$  Signaturen und  $\varphi_i$  eine  $\text{FO}[\sigma_i]$ -Formel, für jedes  $i \in \{1, 2\}$ .

Die Formel  $\varphi_2$  heißt *erfüllbarkeitsäquivalent* zu  $\varphi_1$ , falls gilt:

$$\varphi_2 \text{ ist erfüllbar} \iff \varphi_1 \text{ ist erfüllbar.}$$

**Satz 4.52** (Skolemisierung). *Zu jeder Signatur  $\sigma$  gibt es eine Signatur  $\hat{\sigma}$ , so dass jede  $\text{FO}[\sigma]$ -Formel  $\varphi$  in einen zu  $\varphi$  erfüllbarkeitsäquivalenten gleichheitsfreien  $\text{FO}[\hat{\sigma}]$ -Satz  $\hat{\varphi}$  in Skolemform transformiert werden kann.*

Bevor wir den Satz beweisen, betrachten wir zunächst ein Beispiel.

**Beispiel 4.53.** Die Formel  $\forall x \exists y \forall z \exists u R(x, y, z, u)$  ist erfüllbarkeitsäquivalent zum folgenden gleichheitsfreien Satz in Skolemform:

$$\forall x \forall z R(x, f(x), z, g(x, z))$$

*Beweis von Satz 4.52:*

Wir gehen in mehreren Schritten vor.

*Schritt 1: Elimination von freien Variablen*

Sei  $\{x_1, \dots, x_n\} = \text{frei}(\varphi)$ , seien  $c_1, \dots, c_n$  paarweise verschiedene Konstantensymbole, die nicht in  $\sigma$  liegen.

Sei  $\sigma_1 := \sigma \cup \{c_1, \dots, c_n\}$ , und sei  $\varphi_1$  der FO[ $\sigma_1$ ]-Satz, der aus  $\varphi$  entsteht, indem jedes freie Vorkommen der Variable  $x_i$  (für  $i \in [n]$ ) ersetzt wird durch die Konstante  $c_i$ . Offensichtlicherweise gilt:

$$\varphi_1 \text{ ist erfüllbar} \iff \varphi \text{ ist erfüllbar.}$$

*Schritt 2: Elimination des Gleichheitszeichens*

Sei  $\sigma_2 := \sigma_1 \cup \{G\}$ , wobei  $G$  ein 2-stelliges Relationssymbol ist, das nicht in  $\sigma_1$  vorkommt.

Falls  $\varphi_1$  kein Gleichheitszeichen enthält, so setze  $\varphi_2 := \varphi_1$  und beende Schritt 2. Ansonsten gehe wie folgt vor.

Sei  $\varphi_G$  die Formel, die aus  $\varphi_1$  entsteht, indem jede atomare Subformel der Form  $t_1=t_2$  (für  $\sigma$ -Terme  $t_1, t_2$ ) ersetzt wird durch die Formel  $G(t_1, t_2)$ .

Sei  $\chi_{\text{Äq}}$  ein FO[ $\{G\}$ ]-Satz, der besagt, dass  $G$  eine Äquivalenzrelation ist, d.h.:

$$\begin{aligned} \chi_{\text{Äq}} := & \quad \forall x G(x, x) \quad \wedge \\ & \quad \forall x \forall y (G(x, y) \rightarrow G(y, x)) \quad \wedge \\ & \quad \forall x \forall y \forall z \left( (G(x, y) \wedge G(y, z)) \rightarrow G(x, z) \right). \end{aligned}$$

Für jedes Funktionssymbol  $f \in \sigma$  und für  $k := \text{ar}(f)$  sei  $\chi_f$  der folgende FO[ $\{f, G\}$ ]-Satz, der besagt, dass  $G$  „verträglich“ ist mit  $f$ .

$$\chi_f := \quad \forall x_1 \cdots \forall x_k \forall y_1 \cdots \forall y_k \left( \bigwedge_{i=1}^k G(x_i, y_i) \rightarrow G(f(x_1, \dots, x_k), f(y_1, \dots, y_k)) \right).$$

Für jedes Relationssymbol  $R \in \sigma$  und für  $k := \text{ar}(R)$  sei  $\chi_R$  der folgende FO[ $\{R, G\}$ ]-Satz, der besagt, dass  $G$  „verträglich“ ist mit  $R$ .

$$\chi_R := \quad \forall x_1 \cdots \forall x_k \forall y_1 \cdots \forall y_k \left( \left( \bigwedge_{i=1}^k G(x_i, y_i) \wedge R(x_1, \dots, x_k) \right) \rightarrow R(y_1, \dots, y_k) \right).$$

Sei nun

$$\varphi_2 := \varphi_G \wedge \chi_{\text{Äq}} \wedge \bigwedge_{f \in \sigma(\varphi_1)} \chi_f \wedge \bigwedge_{R \in \sigma(\varphi_1)} \chi_R.$$

Offensichtlicherweise ist  $\varphi_2$  ein gleichheitsfreier  $\text{FO}[\sigma_2]$ -Satz.

*Behauptung:*  $\varphi_2$  ist genau dann erfüllbar, wenn  $\varphi_1$  erfüllbar ist.

*Beweisidee:*

Die Richtung „ $\Leftarrow$ “ ist trivial.

Für den Beweis der Richtung „ $\Rightarrow$ “ sei  $\mathcal{A}$  ein Modell von  $\varphi_2$ . Wir bauen daraus wie folgt ein Modell  $\mathcal{B}$  für  $\varphi_1$ :

Die Elemente des Universums von  $\mathcal{B}$  sind genau die Äquivalenzklassen von Elementen des Universums von  $\mathcal{A}$  bezüglich der Äquivalenzrelation  $G^{\mathcal{A}}$ .

Wir schreiben  $[a]$ , um die Äquivalenzklasse von  $a \in A$  bzgl.  $G^{\mathcal{A}}$  zu bezeichnen, d.h.

$$[a] := \{ a' \in A : (a, a') \in G^{\mathcal{A}} \}.$$

Wir setzen

$$B := \{ [a] : a \in A \}.$$

Für jedes Funktionssymbol  $f \in \sigma$ , für  $k := \text{ar}(f)$  und für alle  $a_1, \dots, a_k \in A$  setzen wir

$$f^{\mathcal{B}}([a_1], \dots, [a_k]) := [f^{\mathcal{A}}(a_1, \dots, a_k)].$$

Wegen  $\mathcal{A} \models \chi_f$  ist dies wohldefiniert.

Für jedes Relationssymbol  $R \in \sigma$  und für  $k := \text{ar}(R)$  setzen wir

$$R^{\mathcal{B}} := \{ ([a_1], \dots, [a_k]) : (a_1, \dots, a_k) \in R^{\mathcal{A}} \}.$$

Wegen  $\mathcal{A} \models \chi_R$  gilt dann für alle  $a'_1, \dots, a'_k \in A$ :

$$([a'_1], \dots, [a'_k]) \in R^{\mathcal{B}} \iff (a'_1, \dots, a'_k) \in R^{\mathcal{A}}.$$

Aus  $\mathcal{A} \models \varphi_G$  kann man nun folgern (Details: Übung), dass gilt:  $\mathcal{B} \models \varphi_2$ . Dies beendet den Beweis der Behauptung.

*Schritt 3: Erzeugen der Formel in Skolemform*

Wir bringen nun den gleichheitsfreien  $\text{FO}[\sigma_2]$ -Satz  $\varphi_2$  in Pränex-Normalform und erhalten dadurch einen zu  $\varphi_2$  äquivalenten gleichheitsfreien  $\text{FO}[\sigma_2]$ -Satz der Form

$$Q_1 x_1 \cdots Q_n x_n \psi,$$

wobei gilt:  $\psi$  ist quantorenfrei und gleichheitsfrei,  $n \geq 0$ ,

$Q_1, \dots, Q_n \in \{\exists, \forall\}$ , und o.B.d.A. sind die Variablen  $x_1, \dots, x_n$  paarweise

verschieden und es gilt  $Q_1 = \forall$  (falls letzteres nicht der Fall ist, ersetzen wir  $\varphi'_2$  durch die Formel  $\forall z \varphi'_2$ , wobei  $z \in \text{VAR} \setminus \{x_1, \dots, x_n\}$ ). Falls  $Q_1 = \dots = Q_n = \forall$  ist, so sind wir fertig. Andernfalls sei  $i \geq 1$  minimal, so dass  $Q_{i+1} = \exists$ . Dann ist  $\varphi'_2$  von der Form

$$\forall x_1 \dots \forall x_i \exists x_{i+1} \xi$$

für  $\xi := Q_{i+2}x_{i+2} \dots Q_n x_n \psi$ .

Sei  $f$  ein  $i$ -stelliges Funktionssymbol, das nicht zu  $\sigma_2$  gehört. Sei  $\xi'$  die Formel, die aus  $\xi$  entsteht, indem jedes Vorkommen der Variablen  $x_{i+1}$  ersetzt wird durch den Term  $f(x_1, \dots, x_i)$ , sei  $\sigma_{3,1} := \sigma_2 \cup \{f\}$  und sei

$$\varphi_{3,1} := \forall x_1 \dots \forall x_i \xi'$$

*Behauptung:*  $\varphi_{3,1}$  ist genau dann erfüllbar, wenn  $\varphi_2$  erfüllbar ist.

*Beweis:* Übung.

Falls  $\varphi_{3,1}$  keinen Existenzquantor enthält, sind wir fertig und setzen  $\hat{\sigma} := \sigma_{3,1}$  und  $\hat{\varphi} := \varphi_{3,1}$ .

Ansonsten verfahren wir mit  $\varphi_{3,1}$  genauso wie mit  $\varphi'_2$ , um den ersten in  $\varphi_{3,1}$  vorkommenden Existenzquantor zu eliminieren. Nach weniger als  $n$  Iterationen erhalten wir einen zu  $\varphi'_2$  erfüllbarkeitsäquivalenten, gleichheitsfreien Satz in Skolemform. Dies beendet den Beweis von Satz 4.52. □

## 4.6 Automatische Theorembeweiser

Folie 361

### Einfaches Verfahren (ohne Unifikation)

Seien  $\varphi$  und  $\psi$  zwei FO[ $\sigma$ ]-Formeln.

*Ziel:* Automatischer Beweis, dass  $\varphi \models \psi$  gilt.

Dazu reicht es, zu zeigen, dass die Formel  $(\varphi \wedge \neg\psi)$  unerfüllbar ist.

#### Verfahren:

1. Erzeuge einen zu  $(\varphi \wedge \neg\psi)$  erfüllbarkeitsäquivalenten gleichheitsfreien FO[ $\hat{\sigma}$ ]-Satz  $\chi$  in Skolemform (über der erweiterten Signatur  $\hat{\sigma}$ ).  
Nutze dazu das im Beweis von Satz 4.52 vorgestellte Verfahren.
2. Verwende das auf Seite 233 beschriebene Semi-Entscheidungsverfahren, um zu herauszufinden, ob  $\chi$  unerfüllbar ist.

**Beispiel 4.54.**

Sei  $\sigma := \{R/1, c, f/1\}$ ,

$$\begin{aligned}\varphi &:= R(c) \wedge \forall x \exists y ((R(x) \rightarrow R(f(f(y)))) \vee R(f(x))) \\ \psi &:= \exists x R(f(f(x))).\end{aligned}$$

Dann ist  $(\varphi \wedge \neg\psi) =$

$$R(c) \wedge \forall x \exists y ((R(x) \rightarrow R(f(f(y)))) \vee R(f(x))) \wedge \neg\exists x R(f(f(x)))$$

ein gleichheitsfreier Satz. Eine Umformung in Pränex-Normalform liefert den dazu äquivalenten Satz

$$\forall x \exists y \left( R(c) \wedge (\neg R(x) \vee R(f(f(y))) \vee R(f(x))) \wedge \neg R(f(f(x))) \right).$$

Wir erweitern die Signatur um ein 1-stelliges Funktionssymbol  $g$  und erhalten den dazu erfüllbarkeitsäquivalenten gleichheitsfreien Satz in Skolemform  $\chi =$

$$\forall x \left( R(c) \wedge (\neg R(x) \vee R(f(f(g(x)))) \vee R(f(x))) \wedge \neg R(f(f(x))) \right)$$

über der Signatur  $\hat{\sigma} = \{R, c, f, g\}$ .

Für jeden Grundterm  $t \in \text{GT}_{\hat{\sigma}}$  enthält die aussagenlogische Variante  $\text{AHE}(\chi)$  der Herbrand-Expansion von  $\chi$  die aussagenlogische Formel

$$\xi_t := X_{R(c)} \wedge \left( \neg X_{R(t)} \vee X_{R(f(f(g(t))))} \vee X_{R(f(t))} \right) \wedge \neg X_{R(f(f(t)))}.$$

Wir zählen die Grundterme in  $\text{GT}_{\hat{\sigma}}$  in der folgenden Reihenfolge auf

$$t_1 = c, \quad t_2 = f(c), \quad t_3 = g(c), \quad t_4 = f(f(c)), \quad t_5 = g(f(c)), \quad \dots$$

und zählen die Formeln in  $\text{AHE}(\chi)$  in derselben Reihenfolge auf, also

$$\xi_1 = \xi_{t_1}, \quad \xi_2 = \xi_{t_2}, \quad \xi_3 = \xi_{t_3}, \quad \dots$$

Bei dem auf Seite 233 beschriebenen Verfahren wird dann beispielsweise im Schleifendurchlauf für  $i = 5$  getestet, ob die aussagenlogische Formel

$$(\xi_1 \wedge \xi_2 \wedge \xi_3 \wedge \xi_4 \wedge \xi_5)$$

unerfüllbar ist. Dazu können wir beispielsweise das in Kapitel 2.6 behandelte Resolutionsverfahren oder den in Kapitel 2.7 behandelten DPLL-Algorithmus anwenden.

Folie 364

In unserem Beispiel entspricht die Formel  $(\xi_1 \wedge \dots \wedge \xi_5)$  der Klauselmenge

$\Gamma :=$

$$\begin{aligned} & \{ X_{R(c)} \} , \\ & \{ \neg X_{R(c)} , X_{R(f(f(g(c))))} , X_{R(f(c))} \} , \{ \neg X_{R(f(f(c)))} \} , \\ & \{ \neg X_{R(f(c))} , X_{R(f(f(g(f(c))))} , X_{R(f(f(c)))} \} , \{ \neg X_{R(f(f(f(c))))} \} , \\ & \{ \neg X_{R(g(c))} , X_{R(f(f(g(g(c))))} , X_{R(f(g(c)))} \} , \{ \neg X_{R(f(f(g(c))))} \} \\ & \{ \neg X_{R(f(f(c))} , X_{R(f(f(g(f(f(c))))} , X_{R(f(f(f(c))))} \} , \{ \neg X_{R(f(f(f(f(c))))} \} \\ & \{ \neg X_{R(g(f(c))} , X_{R(f(f(g(g(f(c))))} , X_{R(f(g(f(c))))} \} , \{ \neg X_{R(f(f(g(f(c))))} \} \} \end{aligned}$$

Wir konstruieren eine Resolutionswiderlegung für  $\Gamma$ :

- |      |   |                     |
|------|---|---------------------|
| (1)  | $\{ X_{R(c)} \}$  | in $\Gamma$         |
| (2)  | $\{ \neg X_{R(c)} , X_{R(f(f(g(c))))} , X_{R(f(c))} \}$         | in $\Gamma$         |
| (3)  | $\{ X_{R(f(f(g(c))))} , X_{R(f(c))} \}$                         | Resolvente aus 1,2  |
| (4)  | $\{ \neg X_{R(f(f(g(c))))} \}$                                  | in $\Gamma$         |
| (5)  | $\{ X_{R(f(c))} \}$   | Resolvente aus 3,4  |
| (6)  | $\{ \neg X_{R(f(c))} , X_{R(f(f(g(f(c))))} , X_{R(f(f(c)))} \}$ | in $\Gamma$         |
| (7)  | $\{ X_{R(f(f(g(f(c))))} , X_{R(f(f(c)))} \}$                    | Resolvente aus 5,6  |
| (8)  | $\{ \neg X_{R(f(f(c)))} \}$                                     | in $\Gamma$         |
| (9)  | $\{ X_{R(f(f(g(f(c))))} \}$                                     | Resolvente aus 7,8  |
| (10) | $\{ \neg X_{R(f(f(g(f(c))))} \}$                                | in $\Gamma$         |
| (11) | $\emptyset$   | Resolvente aus 9,10 |

Folie 365

Somit ist  $\Gamma$  unerfüllbar (gemäß Satz 2.59). Das auf Seite 233 angegebene Verfahren hält daher (spätestens) im Schleifendurchlauf für  $i = 5$  mit der Ausgabe „ $\chi$  ist unerfüllbar“ an. Da  $\chi$  erfüllbarkeitsäquivalent zur Formel  $(\varphi \wedge \neg\psi)$  ist, wissen wir also, dass  $\varphi \models \psi$  gilt. Dies beendet Beispiel 4.54.

# Literaturverzeichnis

- [BBS06] Patrick Blackburn, Johan Bos, and Kristina Striegnitz. *Learn PROLOG Now!* Kings College Publications, 2006. Online Version: <http://www.learnprolognow.org/>.
- [Bur98] S. Burris. *Logic for Mathematics and Computer Science*. Prentice Hall, 1998.
- [Cam98] P. J. Cameron. *Sets, Logic and Categories*. Springer, 1998.
- [Ebb03] Heinz-Dieter Ebbinghaus. *Einführung in die Mengenlehre*. Spektrum Akademischer Verlag, 2003. 4. Auflage.
- [EFT07] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. *Einführung in die Mathematische Logik*. Spektrum Akademischer Verlag, 2007. 5. Auflage.
- [FG98] Jörg Flum and Martin Grohe. *Parameterized Complexity Theory*. Springer, 1998.
- [HR04] M. Huth and M. Ryan. *Logic in Computer Science — Modelling and Reasoning About Systems*. Cambridge University Press, 2004.
- [KK06] M. Kreuzer and S. Kühling. *Logik für Informatiker*. Pearson, 2006.
- [Lib04] Leonid Libkin. *Elements of Finite Model Theory*. Springer, 2004.

- [Sch00] Uwe Schöning. *Logik für Informatiker*. Spektrum Akademischer Verlag, 2000. 5. Auflage.
- [Sch18] Nicole Schweikardt. „Logik in der Informatik“, Skript zur gleichnamigen Vorlesung am Institut für Informatik der Humboldt-Universität zu Berlin, 2018. Verfügbar unter <https://www2.informatik.hu-berlin.de/logik/lehre/WS19-20//Logik/>.
- [SS94] Ehud Shapiro and Leon Sterling. *The Art of PROLOG: Advanced Programming Techniques*. MIT Press, 1994. 2. Auflage.
- [vD04] D. van Dalen. *Logic and Structure*. Springer, 2004.