

# Einführung in die Logik

Jürgen Koslowski  
unter Verwendung von Materialien von  
Roland Meyer und  
Thorsten Palm

Theoretical Computer Science  
Technische Universität Braunschweig

SS 2023

[https://www.tcs.cs.tu-bs.de/teaching/Logik\\_SS\\_2023.html](https://www.tcs.cs.tu-bs.de/teaching/Logik_SS_2023.html)

# Teil 0

# Überblick und Voraussetzungen

## 0 Executive Summary

## 1 Mathematische Voraussetzungen

- Relationen und Funktionen zwischen Mengen
- Ordnungen und Hüllenoperatoren
- Verbände und vollständige Verbände

# Kapitel 0

## Executive Summary

# Z@@t Horn

# Die Formalisierung des korrekten Schließens

*Unter welchen Umständen folgt aus der Wahrheit einer Menge von Prämissen auch die Wahrheit einer möglichen **Schlußfolgerung**?*

- ▶ Bei den Prämissen und der potentiellen Schlußfolgerung handelt es sich um **Aussagen**, die **wahr** oder **falsch** sein können;
- ▶ die Analyse derartiger Aussagen zeigt, dass sie in endlich vielen Schritten mittels endlich vieler Bindewörter („und“, „oder“, „nicht“ etc.) und ähnlicher Konstrukte („wenn ... dann“) aus einfacheren, und letztlich nicht weiter zerlegbaren **atomaren** Aussagen aufgebaut sind;
- ▶ allein die „Baupläne“ der auftretenden Aussagen und die Wahrheit bzw. Unwahrheit der atomaren Aussagen entscheiden darüber, ob es sich um eine korrekte Schlußfolgerung handelt; der konkrete Inhalt der atomaren Aussagen ist hierfür irrelevant.

Hier setzt die Formalisierung an, mittels **Algebra** und **Ordnungstheorie**.

# Die Sprache Aussagenlogik

- ▶ Um Probleme beliebiger Größe handhaben zu können, verwenden wir hier einen unbeschränkten Vorrat  $\mathcal{A}$  von **atomaren Formeln** oder **Atomen**; diese Menge sollte **abzählbar unendlich** sein, vergl. ▶ Anhang B. Die Atome werden offiziell mit  $p_i, i \in \mathbb{N}$  bezeichnet, in konkreten Anwendungen aber auch mit  $p, q, r \dots$
- ▶ Eine endlichen Menge  $\mathcal{J}$  sog. **Junktoren** abstrahiert eine gewisse Auswahl von Bindewörtern. Jeder Junktor verbindet eine bestimmte Anzahl von Formeln zu einer neuen Formel; dies liefert eine Abbildung  $\mathcal{J} \xrightarrow{ar} \mathbb{N}$  in die natürlichen Zahlen  $\mathbb{N}$ , **Signatur** genannt.

Es wird sich später im Rahmen der **Semantik** herausstellen, dass unterschiedliche Junktorenmengen im Wesentlichen gleichwertig sein können. Insofern ist die spezifische Wahl von  $\mathcal{J}$  nicht entscheidend.

# Die Syntax der Aussagenlogik

- ▷ Der Aufbau zusammengesetzter aus atomaren Formeln, die sog. **Syntax**, erfolgt nach den Regeln einer **Termalgebra**.
- ▷ Die resultierende abzählbar unendlichen Menge  $\mathcal{F}[\mathcal{A}]$  aller  $\mathcal{J}$ -Formeln über  $\mathcal{A}$  ist **automatisch** mit einer Interpretation aller Junktoren als konkreten Operationen versehen, also eine **Algebra** für  $\mathcal{J} \xrightarrow{ar} \mathbb{N}$ .
- ▷ Termalgebren für gegebene Signaturen spielen in Teil 2 der Vorlesung (Prädikatenlogik) noch eine weitere wesentliche Rolle. Weil der zugehörige **Rekursionssatz** uns oft viel Arbeit erspart, führen wir die entsprechenden Begriffe und Ergebnisse in [▶ Anhang A](#) kurz ein, um bei Bedarf darauf zurückgreifen zu können.
- ▷ Die **Infix-Notation** für binäre Junktoren, eine Stil-Frage (“**syntactic sugar**”), macht die Verwendung von Klammern unverzichtbar; ein Übermaß derselben wird durch **Vereinfachungsregeln** begrenzt.



# Semantik der Aussagenlogik

- ▶ Als **Wahrheitswerte** verwenden wir 0 für „falsch“ und 1 für „wahr“.
- ▶ Die Menge  $\mathbb{B} = \{0, 1\}$  trägt auf kanonische Weise selber die Struktur einer **ar**-Algebra, d.h., alle Junktoren aus  $\mathcal{J}$  lassen sich auf natürliche Weise in  $\mathbb{B}$  interpretieren.

Laut Rekursionsatz läßt sich nun jede **Belegung**  $\mathcal{A} \xrightarrow{\varphi} \mathbb{B}$  der Atome mit Wahrheitswerten **eindeutig** zu einer **Bewertung**  $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$  fortsetzen, einem **ar-Homomorphismus**, der die **ar**-Struktur erhält.

- ▶ Die Erfüllungsrelation  $\mathbf{E} \subseteq \mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}}$  zwischen Formeln  $A$  und Belegungen  $\varphi$  liefert einen **Hüllenoperator** bzgl.  $\subseteq$  auf  $\mathbf{P}(\mathcal{F}[\mathcal{A}])$ :

*$A \in \mathcal{F}[\mathcal{A}]$  gehört zur Hülle von  $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$ , wenn jede Belegung, die alle Formeln in  $\Gamma$  erfüllt, auch  $A$  erfüllt; geschrieben*

$$\Gamma \models A$$

## Drei Verfahren um $\Gamma \models A$ zu überprüfen

Wir wählen  $\Gamma \models A$  als Formalisierung des ursprünglichen Problems und nennen die Elemente der **potentiell unendlichen** Menge  $\Gamma$  wieder **Prämissen**.

Zur Überprüfung der Gültigkeit von  $\Gamma \models A$  kann man wie folgt vorgehen:

- ▷ **semantisch**: Anwendung der Definition, etwa per Wahrheitstabelle (i.A. zeitaufwändig); der sog. **Kompaktheitssatz** erlaubt zumindest die Beschränkung auf endliche Prämissenmengen;
- ▷ **syntaktisch**: Konstruktion von **Kalkülen** auf Formeln mit **syntax-basierten** sog. **Schlußregeln**. Gelingt der Nachweis, dass deren finitäre **Herleitbarkeitsrelation**  $\vdash$  mit  $\models$  übereinstimmt (die Inklusionen  $\vdash \subseteq \models$  bzw.  $\models \subseteq \vdash$  werden als **Korrektheit** bzw. **Vollständigkeit** des Kalküls bezeichnet), kann man  $\vdash$  statt  $\models$  verwenden, was häufig schneller ist als der semantische Nachweis.

Wir werden drei solche Kalküle kennenlernen;

- ▷ **algorithmisch**: Da in der klassischen Logik die doppelte Negation semantisch zur Identität äquivalent ist und  $\neg$  durch  $\rightarrow$  und  $\perp$  ausgedrückt werden kann, ergibt sich wegen des **Deduktionstheorems**:

$$\Gamma \models A \text{ gdw. } \Gamma \models \neg\neg A \text{ gdw. } \Gamma \models \neg A \rightarrow \perp \text{ gdw. } \Gamma \cup \{\neg A\} \models \perp$$

Ob  $\Gamma \cup \{\neg A\}$  **inkonsistent** oder **widersprüchlich** ist läßt sich dann mit diversen **Algorithmen** untersuchen, die in der Praxis häufig schneller sind als die Berechnung einer Wahrheitstabelle.

Während die **Tableau-Methode** auf beliebige Formeln anwendbar ist, erfordert das **Davis-Putnam-Verfahren** Formeln in sog. **Negations-Normalform (NNF)**, und die **Resolutions-Methode** Formeln in sog. **konjunktiver Normalform (KNF)**. Da letztere i.A. nicht effizient berechnet werden kann, behilft man sich mit modifizierten Formeln, die zur Ausgangsformel nicht notwendig äquivalent, aber zumindest **erfüllbarkeitsäquivalent** sind (Stichwort: Tseitin-Transformation).

## Alternative zur klassischen Logik

Der oben skizzierte Zugang zur **klassischen Logik** basiert auf der Idee, Formeln Wahrheitswerte zuzuweisen. Insbesondere ist eine Formel genau dann wahr, wenn sie nicht falsch ist.

Fragt man hingegen, ob man aus konkret vorliegenden Beweisen für die Prämissen einen Beweis für die Schlußfolgerung **konstruieren** kann, so gelten in dieser sog. **konstruktiven** oder **intuitionistischen** Logik strengere Regeln: liegt bisher noch kein Beweis für eine Formel konkret vor, so bedeutet das nicht notwendig, dass keiner existiert, sondern evtl. nur, dass man noch keinen gefunden hat.

Im Kalkül der **natürlichen Deduktion** läßt sich der Unterschied zur klassischen Logik an einer einzigen Schlußregel festmachen, die klassisch erlaubt, aber intuitionistisch verboten ist.

# Logisches Schließen in der Praxis

## Beispiel

Familie Z möchte im kommenden Jahr gern eine Waschmaschine, ein Auto und ein Moped anschaffen. Aber falls Herr Z seinen üblichen Bonus nicht bekommt, können sie sich nicht alles leisten. Die Waschmaschine ist aber unverzichtbar. Und die Familie braucht mindestens ein Fortbewegungsmittel. Wenn sie auch in den Urlaub fahren will, kann sie sich kein Auto leisten. Wenn sie nicht in den Urlaub fährt, muss sie aber ein Moped kaufen, um den Sohn zu besänftigen.

- ▶ Zeigen Sie, dass Familie Z ein Moped und kein Auto anschafft, sofern Herr Z seinen üblichen Bonus nicht bekommt.

## Beispiel (Formalisierung, Teil 1: Ereignisse und Junktoren)

Zunächst wollen wir die relevanten Informationen extrahieren und miteinander in Beziehung setzen:

- ▷ Dazu führen wir für die diversen **Ereignisse**, die eintreten können oder nicht, Abkürzungen ein:
  - $p$  – Erhalt eines Bonusses;
  - $q / r / s$  – Kauf einer Waschmaschine/eines Autos/eines Mopeds;
  - $t$  – Antritt einer Urlaubsreise.
- ▷ Diese verknüpfen wir dann mit passenden logischen **Junktoren**
  - $\neg$  – nicht (Negation) (unär)
  - $\wedge / \vee$  – und / oder (Konjunktion / Disjunktion) (binär)
  - $\rightarrow$  – wenn,dann (Implikation) (binär)

## Beispiel (Formalisierung, Teil 2: die Prämissen)

- „Aber falls Herr Z seinen üblichen Bonus nicht bekommt, können sie sich nicht alles leisten.“

$$B_0 = \neg p \rightarrow \neg(q \wedge r \wedge s)$$

- „Die Waschmaschine ist aber unverzichtbar.“

$$B_1 = q$$

- „Die Familie braucht mindestens ein Fortbewegungsmittel.“

$$B_2 = r \vee s$$

- „Wenn sie in den Urlaub fahren will, kann sie sich kein Auto leisten.“

$$B_3 = t \rightarrow \neg r$$

- „Wenn sie nicht in den Urlaub fährt, muss sie ein Moped kaufen.“

$$B_4 = \neg t \rightarrow s$$

## Beispiel (Formalisierung, Teil 3: die Schlußfolgerung)

Fraglich ist, ob aus der Wahrheit der Prämissen  $B_i$ ,  $i < 5$ , auch die von

- „Sofern Herr Z seinen üblichen Bonus nicht bekommt, schafft Familie Z ein Moped und kein Auto an.“

$$A = \neg p \rightarrow (\neg r \wedge s)$$

folgt, formal geschrieben als

$$\{B_0, B_1, B_2, B_3, B_4\} \models A \quad (*)$$

Anstatt jetzt alle  $2^5 = 32$  Belegungen der Atome  $p$ ,  $q$ ,  $r$ ,  $s$  und  $t$  darauf zu überprüfen, ob sie  $A$  erfüllen, sofern die Prämissen  $B_i$ ,  $i < 5$ , erfüllt werden, kommen wir später auf dieses Problem zurück.

Es wird sich zeigen, dass Bedingung (\*) äquivalent ist zur **Unerfüllbarkeit** der Formelmenge

$$\{B_0, B_1, B_2, B_3, B_4, \neg A\}$$



# Warum Prädikatenlogik?

Die bisherige Aussagenlogik funktioniert für nicht notwendig spezifische atomare Aussagen, die sich mit „wahr“ oder „falsch“ belegen lassen; sie werden dort als “black boxes” behandelt.

Wollen wir aber einen spezifischen Datenbereich genauer analysieren,

- ▷ etwa die natürlichen Zahlen mit ihrer Arithmetik  $0, 1, +, \cdot$ ;
- ▷ oder Typen von Graphen (gerichtet, ungerichtet, Bäume etc.);
- ▷ oder Mengen und Funktionen, oder Relationen;
- ▷ oder Datenbanken mit Update- und Löschoperationen;
- ▷ ...

müssen wir auch die atomare Formel darauf zuschneiden, etwa, indem wir sie mit einer inneren Struktur versehen, die die Gegebenheiten des zu untersuchenden Datenbereichs widerspiegelt.

# Syntax der Prädikatenlogik

- ▶ Eine verallgemeinerte Signatur  $\mathbf{Fun} + \mathbf{Rel} \xrightarrow{\mathcal{S}} \mathbb{N}$  aus formalen Funktions- und Relationssymbolen (**Operatoren** und **Prädikaten**) beschreibt (**hoffentlich**) alle relevanten Aspekte des Datenbereichs (das Symbol  $+$  oben bezeichnet **disjunkte Vereinigung**);
- ▶ Über einer Variablenmenge  $\mathcal{V}$  liefert  $\mathbf{Fun}$  wieder eine Termalgebra.
- ▶ Die neuen atomaren Formeln sind nun Aussagen darüber, ob passende Tupel solcher Terme formal eines der Prädikate erfüllen.
- ▶ Im Fall  $\mathbf{Rel} = \emptyset$  genügt das nicht. Daher betrachtet man immer ein spezielles binären Prädikat  $\doteq$  für formale **Gleichungen**. Dieses soll in der Semantik auch immer als Gleichheit interpretiert werden.
- ▶ Neben den aussagenlogischen Junktoren kommen nun weitere einstellige Junktoren aus mit sog. **Quantoren**  $\forall$  (für alle) und  $\exists$  (es gibt) versehenen Variablen zum Einsatz, die ihre jeweiligen Variablen in ihrem Geltungsbereich **binden** (Achtung: potentielle Fehlerquelle!).

# Semantik der Prädikatenlogik

- ▷ Die Semantik spielt sich nun in  **$\mathcal{S}$ -Strukturen** ab, d.h., Mengen mit einer Interpretation der Funktions- und Relationssymbole aus  $\mathcal{S}$ .
- ▷ Um die semantischen Begriffsbildungen möglichst eng an die der Aussagenlogik anzulehnen, betrachten wir die  $\mathcal{S}$ -Strukturen zunächst als **Parameter**; ein Durchschnitt über alle  $\mathcal{S}$ -Strukturen liefert dann davon unabhängige Begriffe.
- ▷ Eine ebenfalls weit verbreitete alternative Beschreibung der Semantik läßt sich mit Hilfe eines mathematischen Tricks (Curry/Uncurry) aus der hier eingeführten gewinnen; dabei geht allerdings die enge Analogie zur Aussagenlogik verloren.

Die Äquivalenz zwischen logischer Folgerung  $\Gamma \models A$  und der Unerfüllbarkeit der Menge  $\Gamma \cup \{\neg A\}$  bleibt in der Prädikatenlogik erhalten.

- ▷ Die Charakterisierung erfüllbarer Formelmengen vereinfacht sich, wenn neue Normalformen im Hinblick auf die neuen Quantoren betrachtet werden. Wie schon in der Aussagenlogik ([Tseitin-Transformation](#)) rückt auch hier bei der sog. [Skolemisierung](#) die Abschwächung der Äquivalenz von Formeln zur sog. [Erfüllbarkeitsäquivalenz](#) in den Fokus.
- ▷ Dies dient zur Vorbereitung der Sätze von [Herbrand](#) und von [Löwenheim-Skolem](#) zur Charakterisierung erfüllbarer Formelmengen. Weiter impliziert letzterer die Existenz von Nichtstandardmodellen z.B. der natürlichen Zahlen. Der Satz von [Gödel-Herbrand-Skolem](#) schlägt die Brücke zur Aussagenlogik und eröffnet mit dem Algorithmus von Gilbert die Möglichkeit, Tableaus und die Resolutionsmethode an die Gegebenheiten der Prädikatenlogik anzupassen, und andererseits einen Kompaktheitssatz für diese mit Hilfe der aussagenlogischen Version zu beweisen.

# Kapitel 1

## Mathematische Voraussetzungen

## Mengen naiv betrachtet

Wir betrachten Mengen zunächst naiv als Zusammenfassungen konkreter oder abstrakter Objekte; die grundlegende Relation  $\in$  sagt aus, ob ein Objekt  $x$  zur Menge  $A$  gehört oder nicht:

$$x \in A \quad \text{bzw.} \quad x \notin A$$

Weiter bezeichnet  $|A|$  die Anzahl der Elemente von  $A$ .

Solange die Beschreibung der zusammengefassten Objekte nicht selbst-referentiell ist, treten keine Problem auf:

### Beispiel

Die Mengen  $A$ , die sich nicht selber als Element enthalten, also  $A \notin A$  erfüllen, kann man **nicht** zu einer Menge zusammenfassen.

Wir unterscheiden endliche Mengen, wie die **leere Menge**  $\emptyset$  oder die drei-elementige Menge  $\{a, b, c\}$ , von unendlichen Mengen, wie den natürlichen Zahlen  $\mathbb{N} := \{0, 1, 2, 3, \dots\}$  oder den reellen Zahlen  $\mathbb{R}$ .

# Operationen auf Mengen

## Definition

Eine Menge  $A$  heißt **Teilmenge** einer Menge  $B$  (und entsprechend  $B$  **Obermenge** von  $A$ ), wenn aus  $x \in A$  folgt  $x \in B$ ; Schreibweise  $A \subseteq B$ .

## Definition

Für je zwei Objekte  $a$  und  $b$  bezeichnet  $\langle a, b \rangle$  deren **geordnetes Paar**; im Gegensatz zur Menge  $\{a, b\} = \{b, a\}$  genügt es der Spezifikation

$$\langle a, b \rangle = \langle c, d \rangle \quad \text{gdw.} \quad a = c \quad \text{und} \quad b = d$$

## Definition

Für zwei Mengen  $A$  und  $B$  definiert man

- ▷ den **Durchschnitt**  $A \cap B := \{x : x \in A \text{ und } x \in B\}$ ;
- ▷ die **Vereinigung**  $A \cup B := \{x : x \in A \text{ oder } x \in B\}$ ;
- ▷ das **cartesische Produkt**  $A \times B := \{\langle a, b \rangle : a \in A \text{ und } b \in B\}$ .

$B^n$  bezeichnet das  $n$ -fache cartesische Produkt einer Menge  $B$  mit sich selbst, die Elemente heißen  **$n$ -Tupel** oder **Wörter der Länge  $n$** .  
 Beachte: es gibt jeweils genau ein  $0$ -Tupel  $\varepsilon_B \in B^0$ , das sog. **leere Wort**.

### Definition

Für eine Menge  $B$  definiert man

- ▷ die **Potenzmengen**  $P(B) := \{A : A \subseteq B\}$  und  $P_\omega(B) := \{A : A \subseteq B \text{ endlich}\}$ ;
- ▷ die Menge aller **Wörter**  $B^* := \bigcup_{n \in \mathbb{N}} B^n$  (automatisch disjunkt!).

### Definition

Sind  $A$  und  $B$  Mengen, so heißt eine Teilmenge  $R \subseteq A \times B$  auch (**binäre**) **Relation von  $A$  nach  $B$** ; Schreibweise in dieser VL:  $A \xrightarrow{R} B$ .

Die **duale Relation**  $B \xrightarrow{R^{\text{op}}} A$  besteht genau aus den geordneten Paaren  $\langle b, a \rangle \in B \times A$ , die  $\langle a, b \rangle \in R$  erfüllen. Offenbar gilt  $(R^{\text{op}})^{\text{op}} = R$ .

Statt  $\langle a, b \rangle \in R$  schreibt man auch  $aRb$  (**Infix-Notation**), z.B. für  $\leq$ .



# Wichtige binäre Relationen auf einer Menge $B$

## Definition

Eine Relation  $B \xrightarrow{R} B$  heißt

- ▷ **reflexiv**, falls  $xRx$  für alle  $x \in B$ ;
- ▷ **transitiv**, falls aus  $xRyRz$  folgt  $xRz$  für alle  $x, y, z \in B$ ;
- ▷ **symmetrisch**, falls aus  $xRy$  folgt  $yRx$  für alle  $x, y \in B$ ;
- ▷ **anti-symmetrisch**, falls aus  $xRyRz$  folgt  $x = y$  für alle  $x, y \in B$ ;
- ▷ **total**, falls  $xRy$  oder  $yRx$  gilt für alle  $x, y \in B$ ;
- ▷ **Äquivalenzrelation**, falls  $R$  reflexiv, transitiv und symmetrisch ist;
- ▷ **Quasiordnung**, falls  $R$  reflexiv und transitiv ist;
- ▷ **Halbordnung**, falls  $R$  reflexiv, transitiv und anti-symmetrisch ist.

HA.

Welche dieser Eigenschaften bleiben unter Durchschnitten erhalten?

# Funktionen als spezielle Relationen und Komposition

## Definition

Eine Relation  $A \xrightarrow{f} B$  heißt

- (a) **voll**, wenn zu jedem  $a \in A$  ein  $b \in B$  existiert mit  $afb$ ;
- (b) **partielle Funktion** oder **einwertig**, wenn aus  $afb$  und  $afc$  folgt  $b = c$ ;
- (c) **Funktion**, wenn sie voll und einwertig ist.

Schreibweise:  $A \xrightarrow{f} B$  und  $f(a)$  für das eindeutige  $b \in B$  mit  $afb$ . Die Menge aller Funktionen von  $A$  nach  $B$  wird mit  $B^A$  bezeichnet.

Identifiziert man  $n \in \mathbb{N}$  mit  $\{0, 1, \dots, n-1\}$ , so sind die obigen  $n$ -Tupel in  $B$  nichts weiter als Funktionen von  $n$  nach  $B$ .

## Definition

Die **Komposition**  $A \xrightarrow{R; S} C$  (alternativ:  $S \circ R$ ) für  $A \xrightarrow{R} B \xrightarrow{S} C$  ist gegeben durch:  $a(R; S)c$  gdw. ein  $b \in B$  existiert mit  $aRbSc$ . Hier spielt die **Identitätsfunktion**  $id_B := \{\langle b, b \rangle : b \in B\}$  eine besondere Rolle (s.u.).

# Elementfreie Charakterisierung relationaler Eigenschaften

## Lemma (HA.)

Eine Relation  $B \xrightarrow{R} B$  ist genau dann

- ▷ reflexiv, wenn  $\mathbf{id}_B \subseteq R$ ;
- ▷ symmetrisch, wenn  $R \subseteq R^{\text{op}}$ ;
- ▷ transitiv, wenn  $R; R \subseteq R$ ;
- ▷ total, wenn  $R \cup R^{\text{op}} = B \times B$ .

$R^n$  sei die  $n$ -fache Komposition von  $B \xrightarrow{R} B$  mit sich;  $R^0 = \mathbf{id}_B$ .

## Satz

- ▷  $R^+ = \bigcup \{ R^n : n > 0 \}$  die kleinste transitive Relation, die  $R$  enthält, die sog. **transitive Hülle**;
- ▷  $R^* = \bigcup \{ R^n : n \in \mathbb{N} \}$  die kleinste reflexive und transitive Relation, die  $R$  enthält, die sog. **reflexive transitive Hülle**;
- ▷  $R^e = \bigcup \{ (R \cup R^{\text{op}})^n : n \in \mathbb{N} \}$  die kleinste Äquivalenzrelation, die  $R$  enthält, die sog. **Äquivalenz-Hülle**.

# Eigenschaften von Funktionen

## Satz

- 1 Die Komposition von Relationen ist assoziativ mit neutralen Elementen der Form  $\mathbf{id}_B$ ,  $B$  eine Menge.
- 2 Die Funktionen sind unter Komposition abgeschlossen.

## Definition

Eine Funktion  $A \xrightarrow{f} B$  heißt

- ▷ **injektiv**, falls  $f^{\text{op}}$  einwertig ist (aus  $f(a) = f(c)$  folgt  $a = c$ );
- ▷ **surjektiv**, falls  $f^{\text{op}}$  voll ist (zu  $b \in B$  ex.  $a \in A$  mit  $f(a) = b$ );
- ▷ **bijektiv**, wenn  $f$  injektiv und surjektiv ist.

## Satz

Ist  $A \xrightarrow{f} B$  bijektiv, so gilt für die sog. **Umkehrfunktion**  $B \xrightarrow{f^{\text{op}}} A$ :  
 $f; f^{\text{op}} = f^{\text{op}} \circ f = \mathbf{id}_A$  und  $f^{\text{op}}; f = f \circ f^{\text{op}} = \mathbf{id}_B$ .

# Anmerkungen

- ▷ Es besteht eine bijektive Beziehung zwischen **Teilmengen**  $B \subseteq A$  und **charakteristischen Funktionen**  $A \xrightarrow{\chi_B} \mathbb{B} := \{0, 1\} = 2$ , die genau die Elemente von  $B$  auf 1 abbilden.<sup>1</sup> Das führt auch zu der alternativen Bezeichnung  $2^A$  für die  $2^{|A|}$ -elementige Potenzmenge  $\mathbf{P}(A)$ .

Insbesondere stehen Relationen  $A \rightarrow B$ , also Teilmengen von  $A \times B$ , in bijektiver Beziehung zu Funktionen  $A \times B \rightarrow \mathbb{B}$ . Wir werden je nach Bedarf zwischen diesen Sichtweisen wechseln.

- ▷ Manche Autoren mögen keine Relationen  $A \xrightarrow{R} B$  und verwenden stattdessen Funktionen  $A \xrightarrow{R} \mathbf{P}(B)$ , die jedem  $a \in A$  **die Menge**  $\{b \in B : aRb\}$  seiner Bilder zuordnen; diese kann auch leer sein. Das scheint weitgehend eine Geschmacksfrage zu sein.

---

<sup>1</sup>  $\mathbb{B}$  ist ein **subobject classifier** in der Kategorie **set** der Mengen und Funktionen.

# Beispiele für Quasi-/Halb-Ordnungen

## Beispiel

- ▶ Die Gleichheit  $=$  ist sowohl eine Äquivalenzrelation als auch eine Halbordnung auf jeder Menge  $X$ ;
- ▶  $\leq$  ist eine lineare Halb-Ordnung auf  $\mathbb{B}$ ,  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{R}$ ;
- ▶  $\subseteq$  ist eine Halb-Ordnung auf der Potenzmenge  $P(X)$  einer Menge  $X$ , sie ist i.A. nicht linear;
- ▶ die Teilbarkeitsrelation  $|$  ist eine nicht lineare Halbordnung auf  $\mathbb{N}$ ;
- ▶ Jede Abbildung  $X \xrightarrow{f} Y$  induziert eine Äquivalenzrelation auf  $X$  vermöge  $x \sim_f x'$  gdw.  $f(x) = f(x')$  (das sog. **kernel pair**);
- ▶ Jede Abbildung  $X \xrightarrow{f} \langle Y, \leq \rangle$  in eine quasi-geordnete Menge induziert eine Quasi-Ordnung auf  $X$  vermöge  $x \sqsubseteq_f x'$  gdw.  $f(x) \leq f(x')$ , was  $f$  zu einer monotonen Abbildung (s.u.) macht ( $\sqsubseteq_f$  ist ein sog. **comma object**).

# Polaritäten

## Definition

Eine Abbildung  $\langle X, \leq \rangle \xrightarrow{f} \langle Y, \sqsubseteq \rangle$  zwischen quasi-geordneten Mengen heißt **monoton**, bzw. **antiton**, falls für alle  $a, b \in X$

$$a \leq b \text{ impliziert } f(a) \sqsubseteq f(b) \text{ bzw. } f(b) \sqsubseteq f(a)$$

## Satz

Jede Relation  $X \xrightarrow{R} Y$  induziert zwei antitone Abbildungen (**Polarität**)

$$\langle P(X), \subseteq \rangle \begin{array}{c} \xleftarrow{R^\triangleleft} \\ \xrightarrow{R^\triangleright} \end{array} \langle P(Y), \subseteq \rangle \quad \text{via} \quad \begin{array}{l} R^\triangleleft(V) = V^\triangleleft := \{x \in X : xRV\} \\ R^\triangleright(U) = U^\triangleright := \{y \in Y : URy\} \end{array}$$

die zudem beide beliebige Vereinigungen in Durchschnitte abbilden.  
Weiter gilt für alle  $U \subseteq X$  und alle  $V \subseteq Y$

$$U \subseteq V^\triangleleft \text{ gdw. } V \subseteq U^\triangleright \text{ also auch } V^{\triangleleft\triangleright} = V^\triangleleft \text{ sowie } U^{\triangleright\triangleleft} = U^\triangleright \quad \square$$

# Hüllenoperatoren

## Definition

Eine monotone Abbildung  $\langle X, \leq \rangle \xrightarrow{H} \langle X, \leq \rangle$  heißt **Hüllenoperator**, falls

- ▷  $H$  **extensiv** ist, d.h.  $x \leq H(x)$  für alle  $x \in X$ ;
- ▷  $H$  **idempotent** ist, d.h.,  $H(H(x)) \leq H(x)$  für alle  $x \in X$ .

Im halb-geordneten Fall gilt wegen der Monotonie  $H(H(x)) = H(x)$ .

## Satz

Für jedes  $R \subseteq X \times Y$  ist  $R^\triangleright; R^\triangleleft$  und  $R^\triangleleft; R^\triangleright$  ein Hüllenoperator auf  $P(X)$  bzw.  $P(Y)$ .

## Beweis.

Wegen  $U^\triangleright \subseteq U^\triangleright$  gdw.  $U \subseteq U^{\triangleright\triangleleft}$  ist  $R^\triangleright; R^\triangleleft$  extensiv; analog für  $R^\triangleleft; R^\triangleright$ . Die Idempotenz von  $R^\triangleright; R^\triangleleft$  folgt sofort aus  $U^\triangleright = U^{\triangleright\triangleleft}$ , was  $U^{\triangleright\triangleleft} = U^{\triangleright\triangleleft\triangleright}$  impliziert; analoges gilt für  $R^\triangleleft; R^\triangleright$ . □



# Hüllenoperatoren auf vollständigen Verbänden

## Definition

In einer quasi-geordneten Menge  $\langle X, \sqsubseteq \rangle$  heißt  $x \in X$  **untere Schranke** von  $Q \subseteq X$  falls  $x \sqsubseteq q$  für alle  $q \in Q$  gilt.

Hat jede (jede endliche) Teilmenge  $Q \subseteq X$  eine größte untere Schranke  $\sqcap Q$  ( $\sqcap Q$ ), das **Infimum** von  $Q$ , so heißt  $\langle X, \sqsubseteq \rangle$   **$\sqcap$ -( $\sqcap$ -)Halbverband**.

DUALE BEGRIFFE: **obere Schranke**,  **$\sqcup$ -( $\sqcup$ -)Halbverband**

In einem (**vollständigen**) **Verband** hat jede endliche (jede) Teilmenge ein Infimum und ein Supremum.

## Beispiel

- ▷ Jede linear geordnete Menge ist ein Verband;  $\sqcap = \min$ ,  $\sqcup = \max$ .
- ▷ Jede Potenzmenge ist ein vollständiger Verband;  $\sqcap = \cap$ ,  $\sqcup = \cup$ .
- ▷  $\mathbb{N}$  ist ein Verband bzgl.  $|$ ; dabei gilt  $\sqcap = \mathbf{ggT}$  und  $\sqcup = \mathbf{kgV}$ .

## Satz

Ist  $\langle X, \sqsubseteq \rangle$  ein (vollständiger) Verband, und ist  $\mathcal{H} = \langle H_i : i \in I \rangle$  eine Familie von Hüllenoperatoren auf  $\langle X, \sqsubseteq \rangle$  mit  $I$  beliebig(!), so ist auch  $\bigcap \mathcal{H}$  ein Hüllenoperator mit

$$\bigcap \mathcal{H}(x) = \bigcap \{ H_i(x) : i \in I \}$$

## Beweis

**Monotonie:** Für  $x \sqsubseteq y$  in  $X$  gilt  $H_i(x) \sqsubseteq H_i(y)$  für alle  $i \in I$  und daher  $\bigcap \{ H_i(x) : i \in I \} \sqsubseteq \bigcap \{ H_i(y) : i \in I \}$ .

**Extensivität:** Aus  $x \sqsubseteq H_i(x)$  für  $i \in I$  folgt  $x \sqsubseteq \bigcap \mathcal{H}$ .

**Idempotenz:**  $\bigcap \mathcal{H}(x) \sqsubseteq H_i(x)$  für  $x \in X$  und  $i \in I$  impliziert

$$H_i(\bigcap \mathcal{H}(x)) \sqsubseteq H_i(H_i(x)) = H_i(x) \text{ also } \bigcap \mathcal{H}(\bigcap \mathcal{H}(x)) \sqsubseteq \bigcap \mathcal{H}(x) \quad \square$$

Beachte: da es nur eine Menge von Hüllenoperatoren auf  $\langle X, \sqsubseteq \rangle$  gibt, darf der Index  $i$  sogar eine **echte Klasse** durchlaufen! Diese Tatsache nutzen wir bei der Definition der logischen Folgerung  $\models$  der Prädikatenlogik aus.

# Teil 1

## Aussagenlogik (AL)

# Inhaltsverzeichnis, Teil 1

- 2 Syntax
- 3 Semantik
  - Elementare Definitionen
  - Der Kompaktheitssatz
  - Formeln modulo Äquivalenz
- 4 Deduktion allgemein
- 5 Hilbert-Kalkül
- 6 Natürliche Deduktion und Sequenzen-Kalkül
- 7 Algorithmen
  - Semantische Tableaus: Praxis
  - Semantische Tableaus: Theorie
  - Normalformen
  - Davis-Putnam-Verfahren
  - Resolution
  - Tseitin-Transformation

# Kapitel 2

## Syntax

# Die Sprache der AL verwendet drei Sorten von Symbolen:

- ▷ Ein abzählbar unendlicher Vorrat  $\mathcal{A}$  von **Aussagen-Variablen** oder **atomaren Formeln**  $p, q, p_i, q_j$  etc., um immer von den relevanten konkreten Aussagen abstrahieren zu können;
- ▷ Abstraktionen der Bindewörter „und“, „oder“, „nicht“ etc. der natürlichen Sprache mittels einer endlichen Menge  $\mathcal{J}$  sog. **Junktoren**, deren Namen die intendierte Semantik (s.u.) andeuten, unter anderem

$\wedge$	<b>Konjunktion</b>	für „und“
$\vee$	<b>Disjunktion</b>	für „oder“
$\rightarrow$	<b>Implikation</b>	für „[wenn...], dann“
$\leftrightarrow$	<b>Äquivalenz</b>	für „genau dann wenn“
$\neg$	<b>Negation</b>	für „nicht“
$\top$	<b>Gewissheit</b>	für „wahr“
$\perp$	<b>Absurdität</b>	für „falsch“

- ▷ ggf. Klammern ( und ) zum Auflösen eventueller Mehrdeutigkeiten.

## Stelligkeit der Junktoren und Rolle der Klammern

Die Anzahl der zu verbindenden Aussagen durch die Bindewörter weist den sie abstrahierenden Junktoren eine **endliche Stelligkeit** zu:

nullär:  $\perp$  und  $\top$  ; unär:  $\neg$  ; binär:  $\wedge, \vee, \rightarrow, \leftrightarrow$  .

**ar** (engl. “arity”) bezeichnet die entsprechende Abbildung von der Menge  $\mathcal{J} = \{\perp, \top, \neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$  in die Menge  $\mathbb{N} = \{0, 1, 2, \dots\}$  der natürlichen Zahlen; dies ist eine **Signatur** im Sinne von [Anhang A](#) auf  $\mathcal{J}$  .

Die zugehörigen **Terme**, d.h., bestimmte wohlgeformte Wörter über der **disjunkten** (!) Vereinigung  $\mathcal{J}[\mathcal{A}] := \mathcal{J} + \mathcal{A}$ , dem **Alphabet** der AL, heißen hier **Formeln**. Die Infix-Notation für binäre Junktoren erfordert zwingend die Klammern ( und ) im Alphabet, also  $\mathcal{J}^0[\mathcal{A}] := \mathcal{J}[\mathcal{A}] + \{(, )\}$ , derer man bald mit Ersparnis-Regeln Herr zu werden versucht sein wird.

[Da die “(reverse) polish notation” ((R)PN) für Terme ohne Klammern auskommt, sind diese kein echter Bestandteil der Sprache der AL, sondern nur **syntaktischer Zucker**, ein darstellungstechnisches Artefakt ohne inhärent logische Bedeutung.]

# Die formale Sprache der AL: Formeln

## Definition (induktiv, Infix-Version)

Die formale **Sprache**  $\mathcal{F}[\mathcal{A}]$  der AL ist die **kleinste** Menge von Wörtern über dem Alphabet  $\mathcal{J}^0[\mathcal{A}]$  mit folgenden **Abschlusseigenschaften**:

- ▷  $\mathcal{A} \cup \{\perp, \top\} \subseteq \mathcal{F}[\mathcal{A}]$ ;
- ▷ wenn  $A \in \mathcal{F}[\mathcal{A}]$ , dann  $\neg A \in \mathcal{F}[\mathcal{A}]$ ;
- ▷ wenn  $A, B \in \mathcal{F}[\mathcal{A}]$ , dann  $(A \star B) \in \mathcal{F}[\mathcal{A}]$  mit  $\star$  binär.

Die Elemente von  $\mathcal{F}[\mathcal{A}]$  heißen **Formeln**; diejenigen mit mindestens einem Junktor heißen **molekular** (im Unterschied zu den atomaren Formeln in  $\mathcal{A}$ ). Der letzter Junktor bei der Konstruktion einer Formel heißt **Hauptjunktor**.

Dies ist im Wesentlichen die Definition der Terme aus ▶ Anhang A für die konkrete Signatur  $\mathcal{J} \xrightarrow{\text{ar}} \mathbb{N}$ , wobei für binäre Junktoren statt der polnischen Notation  $\star A B$  oder, besser lesbar,  $\star(A, B)$ , die zwingend Klammer-bewehrte Infix-Schreibweise  $(A \star B)$  verwendet wird.



## Alternative Beschreibung: Formeln via BNF

Informatiker drücken den Aufbau generischer Formeln  $\mathbf{F}$  gern **rekursiv** mit Hilfe einer „Grammatik“ in **Backus-Naur-Form**, kurz **BNF**, aus:

$$\mathbf{F} ::= \mathcal{A} \mid \perp \mid \top \mid \neg \mathbf{F} \mid (\mathbf{F} \star \mathbf{F}) \quad \text{für } \star \text{ binär} \quad (*)$$

Interpretiere die rechte Seite als Mengen-Operation in der Variablen  $\mathbf{F}$ :

- ▷ die senkrechten Striche  $\mid$  bedeuten disjunkte Vereinigung  $+$ ;
- ▷  $\perp$  und  $\top$  stehen für die Singletons  $\{\perp\}$  bzw.  $\{\top\}$ ;
- ▷  $\neg \mathbf{F}$  steht abkürzend für  $\{\neg A : A \in \mathbf{F}\}$ ;
- ▷  $(\mathbf{F} \star \mathbf{F})$  steht abkürzend für  $\{(A \star B) : A, B \in \mathbf{F}\}$ .

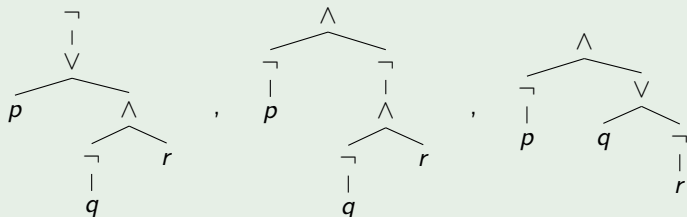
Die Iteration  $\mathbf{F}_0 = \emptyset$ ,  $\mathbf{F}_{n+1} = \mathcal{A} + \{\perp, \top\} + \neg \mathbf{F}_n + (\mathbf{F}_n \star \mathbf{F}_n)$ ,  $\star$  binär, liefert eine streng monoton wachsende Mengen-Folge, deren Vereinigung  $\mathcal{F}[\mathcal{A}] := \bigcup_{i \in \mathbb{N}} \mathbf{F}_i$  die kleinste Lösung der **Fixpunkt-Gleichung**  $(*)$  ist.

# Formeln der AL als Syntaxbäume

## Beispiel

$$\neg(p \vee (\neg q \wedge r)) \quad , \quad (\neg p \wedge \neg(\neg q \wedge r)) \quad , \quad (\neg p \wedge (q \vee \neg r))$$

haben folgende Baum-Darstellung:



Die Redundanz in der 2-dimensionalen Darstellung macht Klammern überflüssig. Eine saubere Definition gelabelter „Bäume“ ist leider viel komplexer als die von Formeln und wird hier unterschlagen.

## Beobachtung

- ① Die obige Signatur  $\mathcal{J} \xrightarrow{ar} \mathbb{N}$  wird oft durch Indizierung der aufgelisteten Junktoren in  $\mathcal{J}$  ausgedrückt:

$$\perp/0, \top/0, \neg/1, \wedge/2, \vee/2, \rightarrow/2, \leftrightarrow/2$$

- ② Die kanonische  $\mathcal{J}$ -Algebrastruktur auf  $\mathcal{F}[\mathcal{A}]$  ist gegeben durch

$$\begin{array}{ll} (\mathcal{F}[\mathcal{A}])^0 \xrightarrow{\Phi(\perp)} \mathcal{F}[\mathcal{A}]; & \bullet \mapsto \perp \\ (\mathcal{F}[\mathcal{A}])^0 \xrightarrow{\Phi(\top)} \mathcal{F}[\mathcal{A}]; & \bullet \mapsto \top \\ (\mathcal{F}[\mathcal{A}])^1 \xrightarrow{\Phi(\neg)} \mathcal{F}[\mathcal{A}]; & A \mapsto \neg A \\ (\mathcal{F}[\mathcal{A}])^2 \xrightarrow{\Phi(\star)} \mathcal{F}[\mathcal{A}]; & \langle A, B \rangle \mapsto (A \star B) \end{array}$$

Üblicherweise lässt man  $\Phi$  weg.

# Strukturelle Induktion

Das allgemeine Beweisprinzip nimmt hier folgende Form an:

## Satz

*Sei  $E$  eine Eigenschaft, die Formeln haben können oder nicht. Falls*

- ▷ jede atomare Formel Eigenschaft  $E$  hat;*
- ▷  $\perp$  und  $\top$  Eigenschaft  $E$  haben;*
- ▷ mit  $A$  auch  $\neg A$  Eigenschaft  $E$  hat;*
- ▷ mit  $A$  und  $B$  auch  $(A \star B)$  Eigenschaft  $E$  hat ( $\star$  binär)*

*dann hat jede Formel in  $\mathcal{F}[\mathcal{A}]$  die Eigenschaft  $E$ .* □

Andere Beweisprinzipien stehen weiterhin zur Verfügung, wie z.B. Induktion über die Länge von Formeln, oder über die Tiefe des Syntaxbaumes...

## Beispiel für strukturelle Induktion

### Lemma (spezifisch für Infix-Schreibweise)

*Jede Formel in  $\mathcal{F}[\mathcal{A}]$  hat gleich viele öffnende wie schließende Klammern.*

### Beweis.

**Induktionsanfang:** Die Behauptung ist korrekt für Formeln in  $\mathcal{A} \cup \{\perp, \top\}$ .

**Induktionsannahme:** Jede Formel mit weniger Junktoren als die molekulare Formel  $A$  erfülle die Behauptung.

**Induktionsschluss:**  $A$  ist durch genau eine der 5 Abschlussoperationen aus Formeln mit weniger Junktoren entstanden. Die Negation fügt keine Klammern hinzu, während die binären Junktoren je eine öffnende und eine schließende Klammer hinzufügen, was die Gleichheit bewahrt.  $\square$

(Anstelle von Formeln mit weniger Junktoren könnte man auch Formeln mit niedrigerer Baumdarstellung betrachten.)

## Alternativer Beweis.

**Idee:** Buch führen über öffnende bzw. schließende Klammern einer Formel.

Wir setzen die Abbildung

$$\mathcal{J}^0[\mathcal{A}] \xrightarrow{\delta} \mathbb{Z} \quad , \quad x \mapsto \begin{cases} 1 & \text{falls } x = ( ; \\ -1 & \text{falls } x = ) , \\ 0 & \text{sonst} \end{cases}$$

auf ganz  $(\mathcal{J}^0[\mathcal{A}])^*$  fort (nicht nur  $\mathcal{F}[\mathcal{A}]$ ), indem wir definieren

$$\bar{\delta}(a_0 a_1 \dots a_{n-1}) := \sum_{i < n} \delta(a_i)^a$$

$\bar{\delta}$  bestimmt also die Differenz zwischen der Anzahl der öffnenden bzw. schließenden Klammern in einem Wort.

Zu zeigen ist nun, dass für jede Formel  $A \in \mathcal{F}[\mathcal{A}]$  gilt  $\bar{\delta}(A) = 0$ .

<sup>a</sup> Dem liegt die strukturelle Induktion für **Monoide** zugrunde, hier  $\langle \mathbb{Z}, +, 0 \rangle$ , wobei uns die Eindeutigkeit der Fortsetzung an dieser Stelle nicht interessiert.

## Fortsetzung

**Induktionsanfang:** Beachte, dass  $\bar{\delta}$  auf  $\mathcal{A} + \{(\,,\,)\}$  mit  $\delta$  übereinstimmt.

**Induktionsannahme:** Jede Formel mit weniger Junktoren als die molekulare Formel  $A$  erfülle die Behauptung.

**Induktionsschluss:**  $A$  ist durch genau eine der 5 Abschlussoperationen aus Formeln mit weniger Junktoren entstanden.

- ▷ Falls  $A = \neg B$  gilt

$$\bar{\delta}(\neg B) = \delta(\neg) + \bar{\delta}(B) = 0 + \bar{\delta}(B) = 0$$

- ▷ Falls  $A = (B \star C)$  gilt

$$\begin{aligned} \bar{\delta}((B \star C)) &= \delta((\ )) + \bar{\delta}(B) + \delta(\star) + \bar{\delta}(C) + \delta()) \\ &= 1 + 0 + 0 + 0 + (-1) = 0 \end{aligned}$$

Hier haben wir die Assoziativität der Addition ausgenutzt. □

Natürlich bildet  $\bar{\delta}$  auch viele andere Wörter auf 0 ab, z.B.  $w = )p\neg(\wedge.$

# $\mathcal{J}$ -Algebra

Alle wesentlichen Konstruktionen auf der  $\mathcal{J}$ -Algebra  $\mathcal{F}[A]$  werden nun mit Hilfe des **Rekursionssatz** vorgenommen.

## Beispiel

**Länge**  $|A| =$  Anzahl aller  $\mathcal{J}^0[A]$ -Symbole in  $A$ : Verwende

- ▷ die konstante Abbildung  $\mathcal{A} \xrightarrow{1} \mathbb{N}$ ;
- ▷ die folgenden Interpretationen von  $\mathcal{J}$  in  $\mathbb{N}$ :

$$\mathbb{N}^0 \xrightarrow{I(\perp)} \mathbb{N}; \quad \bullet \mapsto 1$$

$$\mathbb{N}^0 \xrightarrow{I(\top)} \mathbb{N}; \quad \bullet \mapsto 1$$

$$\mathbb{N}^1 \xrightarrow{I(\neg)} \mathbb{N}; \quad n \mapsto n + 1$$

$$\mathbb{N}^2 \xrightarrow{I(\star)} \mathbb{N}; \quad \langle n, m \rangle \mapsto n + m + 3$$

Nun ist  $\mathcal{F}[A] \xrightarrow{||} \mathbb{N}$  die eindeutige Fortsetzung von  $\mathcal{A} \xrightarrow{\delta} \mathbb{N}$  zu einem  $\mathcal{J}$ -Homomorphismus nach  $\langle \mathbb{N}, I \rangle$ .



## Beispiel

$\#_p(A)$  bezeichne die Anzahl der Vorkommen des Atoms  $p \in \mathcal{A}$  in  $A$ .  
Eine induktive Definition verwendet etwa

$$\#_p(q) = \begin{cases} 1 & \text{falls } q = p ; \\ 0 & \text{sonst} \end{cases} \quad \text{für } q \in \mathcal{A}$$

$$\#_p(\perp) = \#_p(\top) = 0$$

$$\#_p(\neg B) = \#_p(B)$$

$$\#_p((A \star B)) = \#_p(A) + \#_p(B) \quad \text{für } \star \text{ binär}$$

Die letzten drei Zeilen spezifizieren eine **weitere**  $\mathcal{J}$ -Struktur  $K$  auf  $\mathbb{N}$ :

$$K(\perp) = K(\top) = 0 \text{ (konstant)} \quad , \quad K(\neg) = \mathbf{id}_{\mathbb{N}} \quad , \quad K(\star) = +$$

bzgl. der  $\mathcal{F}[\mathcal{A}] \xrightarrow{\#_p} \mathbb{N}$  dann ein  $\mathcal{J}$ -Homomorphismus ist.

Analog kann man z.B. die Menge  $@(A)$  der in  $A$  vorkommenden Atome definieren (HA).

## Teilformeln (T. Palm)

Die Überprüfung, ob auf der Zielmenge wirklich eine  $\mathcal{J}$ -Struktur vorliegt, darf man nicht vergessen:

### Beispiel

Die endliche Menge  $T(A)$  der Teilformeln von  $A$  enthält neben  $A$  die Teilformeln derjenigen Formel(n), aus denen  $A$  mit Hilfe des letzten Junktors (Wurzel des Syntaxbaumes) konstruiert wurde. Etwa

$$T(q) = \{q\} \text{ für } q \in \mathcal{A}, \quad T(\perp) = \{\perp\}, \quad T(\top) = \{\top\}$$

$$T(\neg B) = \{\neg B\} \cup T(B) = L(\neg)(T(B))$$

$$T((A \star B)) = \{(A \star B)\} \cup T(A) \cup T(B) = T(A) L(\star) T(B) \quad (\star \text{ binär})$$

Aber wenn  $\mathcal{F}[\mathcal{A}] \xrightarrow{T} \mathbf{P}_\omega(\mathcal{F}[\mathcal{A}])$  ein  $\mathcal{J}$ -Homomorphismus sein soll, welche  $\mathcal{J}$ -Struktur  $L$  auf  $\mathbf{P}_\omega(\mathcal{F}[\mathcal{A}])$  liegt ihm zugrunde? Um welche negierte Formel soll etwa  $\Gamma$  ergänzt werden um  $L(\neg)(\Gamma)$  zu liefern?

## Beispiel (Fortsetzung)

Was sich hingegen als  $\mathcal{J}$ -Homomorphismus identifizieren lässt ist die Abbildung  $\mathcal{F}[\mathcal{A}] \xrightarrow{\langle \text{id}, T \rangle} \mathcal{F}[\mathcal{A}] \times \mathbf{P}_\omega(\mathcal{F}[\mathcal{A}])$ . Die Spezifikation

$$\langle \text{id}, T \rangle(q) = \langle q, \{q\} \rangle \quad \text{für } q \in \mathcal{A}$$

$$\langle \text{id}, T \rangle(\perp) = \langle \perp, \{\perp\} \rangle$$

$$\langle \text{id}, T \rangle(\top) = \langle \top, \{\top\} \rangle$$

$$\langle \text{id}, T \rangle(\neg B) = \langle \neg B, \{\neg B\} \cup T(B) \rangle$$

$$\langle \text{id}, T \rangle((A \star B)) = \langle (A \star B), \{(A \star B)\} \cup T(A) \cup T(B) \rangle \quad \text{für } \star \text{ binär}$$

liefert folgende Interpretation  $I$  der Junktoren auf  $\mathcal{F}[\mathcal{A}] \times \mathbf{P}_\omega(\mathcal{F}[\mathcal{A}])$ :

- ▷  $I(\perp) = \langle \perp, \{\perp\} \rangle$  und  $I(\top) = \langle \top, \{\top\} \rangle$ ;
- ▷  $I(\neg)\langle A, \Gamma \rangle = \langle \neg A, \{\neg A\} \cup \Gamma \rangle$ ;
- ▷  $\langle A, \Gamma \rangle I(\star) \langle B, \Delta \rangle = \langle (A \star B), \{(A \star B)\} \cup \Gamma \cup \Delta \rangle$ .

# Substitution

Für Formeln  $A, B \in \mathcal{F}[\mathcal{A}]$  und ein Atom  $p \in \mathcal{A}$  bezeichne  $A[p/B]$  die Formel, die durch simultanes Ersetzen jedes Auftretens von  $p$  in  $A$  durch  $B$  entsteht. Genauer:

## Definition

$\mathcal{F}[\mathcal{A}] \xrightarrow{[p/B]} \mathcal{F}[\mathcal{A}]$  ist die durch den Rekursionssatz eindeutig bestimmte homomorphe Fortsetzung der Abbildung

$$\mathcal{A} \xrightarrow{p/B} \mathcal{F}[\mathcal{A}], \quad q \mapsto \begin{cases} B & \text{falls } q = p \\ q & \text{falls } q \neq p \end{cases}$$

bzgl. der kanonischen  $\mathcal{J}$ -Algebra-Struktur auf  $\mathcal{F}[\mathcal{A}]$ .

- ▷ Falls  $A$  kein Atom  $p$  enthält, stimmt  $A[p/B]$  mit  $A$  überein.
- ▷ Falls  $B$  das Atom  $p$  enthält, kann  $p$  in  $A[p/B]$  weiterhin auftreten; daher ist  $[p/B]$  nicht notwendig idempotent!

# Endlich: Klammerersparnisregeln!

Um Klammern einzusparen, verabreden wir folgende

## Bindungskonventionen

- ▶ Junktoren niedrigerer Stelligkeit binden stärker als solche höherer Stelligkeit.
- ▶  $\wedge$  und  $\vee$  binden gleich stark, aber stärker als  $\rightarrow$  und  $\leftrightarrow$ .
- ▶  $\rightarrow$  und  $\leftrightarrow$  binden gleich stark.
- ▶ binäre Junktoren **assoziieren nach rechts**, d.h.,  $A \star B \star C$  ist als  $A \star (B \star C)$  zu interpretieren (evtl. anders als auf alten Folien!). Für  $(A \star B) \star C$  gib es keine Vereinfachung.

**Achtung:** Im Rahmen der Semantik werden wir später sehen, dass die binären Operatoren  $\wedge$ ,  $\vee$  und  $\leftrightarrow$  auf Formeln **modulo Äquivalenz** tatsächlich assoziativ sein werden; für  $\rightarrow$  ist dies aber nicht der Fall!

# Kapitel 3

## Semantik

# Die $\mathcal{J}$ -Algebra $\mathbb{B} = \{0, 1\}$ der Wahrheitswerte

## Definition

Die **kanonische Interpretation** von  $\mathcal{J}$  in  $\mathbb{B}$  (wir lassen  $I$  weg) ist

$$\begin{array}{llll}
 \mathbb{B}^0 \xrightarrow{\perp} \mathbb{B}; & \bullet \mapsto 0 & \mathbb{B}^2 \xrightarrow{\wedge} \mathbb{B}; & \langle x, y \rangle \mapsto \inf\{x, y\} \\
 \mathbb{B}^0 \xrightarrow{\top} \mathbb{B}; & \bullet \mapsto 1 & \mathbb{B}^2 \xrightarrow{\vee} \mathbb{B}; & \langle x, y \rangle \mapsto \sup\{x, y\} \\
 \mathbb{B}^1 \xrightarrow{\neg} \mathbb{B}; & x \mapsto 1 - x & \mathbb{B}^2 \xrightarrow{\rightarrow} \mathbb{B}; & \langle x, y \rangle \mapsto \leq \langle x, y \rangle \\
 & & \mathbb{B}^2 \xrightarrow{\leftrightarrow} \mathbb{B}; & \langle x, y \rangle \mapsto = \langle x, y \rangle
 \end{array}$$

$\mathcal{J}$ -Homomorphismen  $\mathcal{F}[\mathcal{A}] \rightarrow \mathbb{B}$  heißen **Bewertungen**.

Nach dem [Rekursionsatz](#) erlaubt jede **Belegung** der Variablen  $\varphi \in \mathbb{B}^{\mathcal{A}}$  eine eindeutige homomorphe Fortsetzung zu einer Bewertung  $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$ .

## Definition

$\langle \mathcal{A}, \varphi \rangle \mapsto \hat{\varphi}(\mathcal{A})$  liefert eine **Auswertungsfunktion**  $\mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}} \xrightarrow{E} \mathbb{B}$ , die wir auch als **Erfüllungsrelation**  $E \subseteq \mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}}$  auffassen können.

# Wahrheitstabellen und Auswertung von Formeln

Die kanonische Interpretation von  $\mathcal{J}$  in  $\mathbb{B}$  lässt sich alternativ mittels Wahrheitstabellen darstellen:

⊥		⊤		¬		∧	∨	→	↔
0	1	0	1	0	1	0	1	1	0
1	0	1	0	0	1	0	1	0	0
1	1	1	1	1	1	1	1	1	1

Mit deren Hilfe lassen sich Bewertungen von Formeln aufgrund der Belegung der Variablen besonders einfach bestimmen.

**Beispiel (Bestimme  $\hat{\varphi}(\neg(p \wedge q) \rightarrow r)$  falls  $\varphi(p) = 1$ ,  $\varphi(q) = \varphi(r) = 0$ )**

$$\neg(p \wedge q) \rightarrow r$$

$$\underbrace{\underbrace{\underbrace{1 \quad 0}_{0}}_{1}}_{0}$$

oder in „flacher“ Notation  
(verbirgt die Reihenfolge)

$$\neg(p \wedge q) \rightarrow r$$

$$1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0$$



# Boole'sche Funktionen

## Definition

Die obige Auswertungsstrategie, angewandt auf alle Belegungen der  $n = |\mathcal{A}|$  in  $A$  vorkommenden Atome liefert die **von  $A$  induzierte Boole'sche Funktion**  $\mathbb{B}^n \xrightarrow{e_A} \mathbb{B}$ .

Häufig wird  $e_A$  in Tabellenform angegeben:

## Beispiel

$p$	$q$	$r$	$p \vee q$	$q \rightarrow r$	$(q \leftrightarrow r) \wedge \neg(p \vee \neg r)$
0	0	0	0	1	1
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	1	0	1
1	0	1	1	0	0
1	1	0	1	0	0
1	1	1	1	0	1

Offenbar gibt es höchstens  $2^{2^n}$  viele Boole'sche Funktionen auf  $\mathbb{B}^n$ .

# Polarität und Hüllenoperator für die Erfüllungsrelation $E$

Die Relation  $E \subseteq \mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}}$  liefert eine sog. Polarität, d.h., zwei antitone Abbildungen zwischen den entsprechenden Potenzmengen:

$$P(\mathcal{F}[\mathcal{A}]) \begin{array}{c} \xleftarrow{E^\triangleleft} \\ \xrightarrow{E^\triangleright} \end{array} P(\mathbb{B}^{\mathcal{A}}) \quad \text{mit} \quad \begin{array}{l} \Phi^\triangleleft := E^\triangleleft(\Phi) = \{ A \in \mathcal{F}[\mathcal{A}] : \varphi(A) = 1 \text{ für alle } \varphi \in \Phi \} \\ \Gamma^\triangleright := E^\triangleright(\Gamma) = \{ \varphi \in \mathbb{B}^{\mathcal{A}} : \varphi(A) = 1 \text{ für alle } A \in \Gamma \} \end{array}$$

die zudem beide beliebige Vereinigungen in Durchschnitte abbilden.

Für alle Formelmengen  $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$  und alle Belegungsmengen  $\Phi \subseteq \mathbb{B}^{\mathcal{A}}$  gilt

$$\Gamma \subseteq \Phi^\triangleleft \text{ gdw. } \Gamma^\triangleright \supseteq \Phi \quad \text{und folglich} \quad \Gamma^\triangleright = \Gamma^{\triangleright\triangleleft} \quad \text{sowie} \quad \Phi^\triangleleft = \Phi^{\triangleleft\triangleright}$$

was Hüllenoperatoren  $(\ )^{\triangleright\triangleleft}$  und  $(\ )^{\triangleleft\triangleright}$  auf den jeweiligen Potenzmengen liefert.

*Der Hüllenoperator  $(\ )^{\triangleright\triangleleft}$  auf der Potenzmenge der Formelmenge  $\mathcal{F}[\mathcal{A}]$  bildet die Grundlage für den nun einzuführenden Begriff der **logischen Folgerung**:*

# Logische Folgerung $\models$ , Erfüllbar- und Allgemeingültigkeit

## Definition

Betrachte  $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$  (die Menge der sog. **Prämissen**) und  $A, B \in \mathcal{F}[\mathcal{A}]$ .

- ▷ Falls  $A \in \Gamma^{\triangleright\triangleleft}$ , d.h., jeder Erfüller der Prämissen erfüllt auch  $A$ , schreibt man  $\Gamma \models A$  und sagt „ $A$  folgt logisch aus  $\Gamma$ “.
- ▷  $A$  heißt **allgemeingültig/Tautologie**, wenn jede Belegung  $A$  erfüllt. Schreibweise:  $\models A$  statt  $\emptyset \models A$  bzw.  $A \in \emptyset^{\triangleright\triangleleft} = (\mathbb{B}^{\mathcal{A}})^{\triangleleft}$ .
- ▷  $B$  (bzw.  $\Gamma$ ) heißt **erfüllbar**, falls  $\varphi \in \mathbb{B}^{\mathcal{A}}$  existiert mit  $\hat{\varphi}(B) = 1$  (für jedes  $B \in \Gamma$ ), d.h., falls  $\{B\}^{\triangleright} \neq \emptyset$  (bzw.  $\Gamma^{\triangleright} \neq \emptyset$ ).

Formeln  $A \in \mathcal{F}[\mathcal{A}]$  und Belegungen  $\varphi \in \mathbb{B}^{\mathcal{A}}$  erfüllen  $\varphi(A) \neq \varphi(\neg A)$ , daher zerlegt jedes  $A$  die Belegungsmenge disjunkt:  $\mathbb{B}^{\mathcal{A}} = \{A\}^{\triangleright} + \{\neg A\}^{\triangleright}$ .

## Beobachtung.

$A$  ist genau dann eine Tautologie, wenn  $\neg A$  nicht erfüllbar ist. □

# Charakterisierung der Unerfüllbarkeit von Formelmengen

## Lemma

Folgende Bedingungen sind für eine Formelmenge  $\Gamma \subseteq \mathcal{F}[\mathcal{A}]$  äquivalent:

- (0)  $\Gamma$  ist unerfüllbar, bzw.  $\Gamma^\triangleright = \emptyset$ .
- (1)  $\Gamma \models A$  für alle Formeln  $A$ , bzw.  $\Gamma^{\triangleright\triangleleft} = \mathcal{F}[\mathcal{A}]$ .
- (2)  $\Gamma \models \perp$  bzw.  $\perp \in \Gamma^{\triangleright\triangleleft}$ .
- (3)  $\Gamma \models B$  und  $\Gamma \models \neg B$  bzw.  $\{B, \neg B\} \subseteq \Gamma^{\triangleright\triangleleft}$  für ein  $B \in \mathcal{F}[\mathcal{A}]$ .

## Beweis.

- (0)  $\Rightarrow$  (1): Klar, da die Formeln keine Bedingungen erfüllen müssen.
- (1)  $\Rightarrow$  (2), (3): Trivial.
- (2), (3)  $\Rightarrow$  (0):  $\Gamma^\triangleright = (\Gamma^\triangleright)^{\triangleleft} = (\Gamma^{\triangleright\triangleleft})^\triangleright \subseteq \{\perp\}^\triangleright = \{B, \neg B\}^\triangleright = \emptyset$  aufgrund der Eigenschaften des Hüllenoperators  $(\ )^{\triangleright\triangleleft}$  und der Antitonie von  $(\ )^\triangleright$ .  $\square$

# Das semantische Deduktionstheorem (sDT)

Lemma (sDT; Prämissen lassen sich zwischen  $\models$  und  $\rightarrow$  verschieben)

Für  $\Gamma \subseteq \mathcal{F}[A] \ni A, B$  gilt:  $\Gamma \cup \{A\} \models B$  gdw.  $\Gamma \models A \rightarrow B$ .

Beweis.

( $\Rightarrow$ ): Erfüllt  $\varphi$  die Menge  $\Gamma$ , folgt aus  $\hat{\varphi}(A) = 1$  nach Voraussetzung  $\hat{\varphi}(B) = 1$ , oder es gilt  $\hat{\varphi}(A) \leq \hat{\varphi}(B)$ . Beides impliziert  $\hat{\varphi}(A \rightarrow B) = 1$ .

( $\Leftarrow$ ):  $\psi \in (\Gamma \cup \{A\})^\models = \Gamma^\models \cap \{A\}^\models$  erfüllt  $\Gamma$  und  $A$ , nach Voraussetzung also auch  $A \rightarrow B$ , und wegen  $\hat{\psi}(A) \leq \hat{\psi}(B)$  ebenfalls  $B$ .  $\square$

Korollar

$\{A, A \rightarrow B\} \models B$  bzw.  $\Gamma \cup \{A\}$  unerfüllbar gdw.  $\Gamma \models \neg A$ .

Beweis.

Der 2. Teil verwendet, dass  $\varphi(A \rightarrow \perp) = \varphi(\neg A)$  für alle  $\varphi \in \mathbb{B}^A$ .  $\square$

# Der Kompaktheitssatz (KPS)

Alle bisher eingeführten Begriffe sind entscheidbar, solange die Formelmengen endlich sind: dann kommen nur endlich viele Atome vor und man kann eine endliche Wahrheitstabelle aufstellen. Aber  $\Gamma$  darf unendlich sein.

## Definition

$\Gamma$  heißt **endlich erfüllbar**, wenn jede endliche Teilmenge von  $\Gamma$  erfüllbar ist.

Der folgende zentrale Satz besagt, dass man sich im Wesentlichen auf endliche Formelmengen beschränken kann:

## Satz (Kompaktheitssatz)

$\Gamma$  ist genau dann erfüllbar, wenn  $\Gamma$  endlich erfüllbar ist.

Die Notwendigkeit ist trivial, ebenso die Hinlänglichkeit, falls  $\mathcal{A}$  endlich ist (Kontraposition). Vor dem Beweis der Hinlänglichkeit für unendliches  $\mathcal{A}$  betrachten wir erst eine „Anwendung“ und einige Konsequenzen des KPS.

# Ein Matching-Problem

## Beispiel (Hochzeit im Mittelalter, nach T. Palm)

Alle Junggesellinnen eines Dorfes (Menge  $F$ ) sollen verheiratet werden. Dazu liefern sie alle Listen  $T(f) \subseteq M$  der ihnen genehmen Junggesellen ab. Gesucht ist als Lösung dieses speziellen **Matchingproblems** eine injektive **Auswahlfunktion**  $F \xrightarrow{e} M$  mit  $e(f) \in T(f)$  für alle  $f \in F$ .

Nun stellen wir uns das Dorf unendlich groß vor. Die Junggesellinnen bleiben aber bodenständig und liefern nur endliche Listen  $T(f)$  ab.

**Behauptung:** Das Matching-Problem  $F \xrightarrow{T} \mathbf{P}_\omega(M)$  lösbar, wenn es für jede endliche Teilmenge von  $F$  lösbar ist. (Die Umkehrung ist trivial.)

Der folgende Beweis nimmt einige Aspekte der PL aus Teil 2 vorweg.

Um den KPS anwenden zu können verwenden wir als Atome Symbole

$p_{f,m}$  mit  $f \in F$  und  $m \in T(f)$  „ $f$  und  $m$  heiraten.“

## Beispiel (Fortsetzung)

$\Gamma$  besteht aus drei Komponenten, die verschiedene Aspekte der Problemstellung umsetzen ( $f, f' \in F$ ,  $m, m' \in M$ ):

- ▷ Auswahl-eigenschaft:  $H_f := \bigvee_{m \in T(f)} p_{f,m}$ <sup>a</sup>
- ▷ Funktionalität:  $I_{f,m,m'} := p_{f,m} \rightarrow \neg p_{f,m'}$  mit  $m \neq m'$ ;
- ▷ Injektivität:  $J_{f,f',m} := p_{f,m} \rightarrow \neg p_{f',m}$  mit  $f \neq f'$ .

**Voraussetzung:** Jede Einschränkung des Matchingproblems  $T$  auf eine endliche Teilmenge  $F_0 \subseteq F$  ist lösbar.

**Wir zeigen:** Jede endliche Teilmenge  $\Gamma_0 \subseteq \Gamma$  hat eine erfüllende Belegung.

Für endliches  $\Gamma_0 \subseteq \Gamma$  ist auch die Menge

$$F_* := \{ f \in F : f \text{ tritt als Index in einer Formel aus } \Gamma_0 \text{ auf} \}$$

endlich, denn jede Formel in  $\Gamma_0$  hat nur endlich viele Atome.

<sup>a</sup> Endliche Disjunktion von Atomen; nimmt die Assoziativität von  $\vee$  vorweg



## Beispiel (Fortsetzung)

- ▷ Nach Voraussetzung lässt  $F_*$  mindestens eine Lösung  $e_*$  des eingeschränkten Matching-Problems  $T$  zu.
- ▷ Wiederholt man die Konstruktion von  $\Gamma$  mit  $F_*$  anstelle von  $F$ , liefert dies eine endliche Teilmenge  $\Gamma_* \subseteq \Gamma$ , die  $\Gamma_0$  umfasst.
- ▷ Auswahleigenschaft, Funktionalität und Injektivität der Lösungen  $e_*$  entsprechen genau Belegungen, die  $\Gamma_*$  und damit auch  $\Gamma_0$  erfüllen.

Somit ist die Voraussetzung des KPS gegeben, und  $\Gamma$  ist daher erfüllbar, was wiederum eine Lösung des Matchingproblems  $T$  bedeutet.  $\square$

Man beachte

- wie für ein konkretes Problem maßgeschneiderte atomare Formeln eingeführt wurden, die eine Formalisierung (noch) in der AL erlaubten;
- das geschickte Zusammenspiel von endlichen Formelmengen und endlichen Probleminstanzen.

# Varianten des Kompaktheitssatzes

Korollar (wird auch oft als KPS bezeichnet).

$\Gamma \models A$  genau dann wenn  $\Gamma_0 \models A$  für eine endliche Teilmenge  $\Gamma_0 \subseteq \Gamma$ .

Beweis.

$\Gamma \models A$  gdw.  $\Gamma \cup \{\neg A\}$  unerfüllbar

gdw.  $\Gamma \cup \{\neg A\}$  hat eine endliche unerfüllbare Teilmenge  $\Gamma_1$

gdw.  $\Gamma$  hat eine endliche Teilmenge  $\Gamma_0$  mit  $\Gamma_0 \cup \{\neg A\}$  unerfüllbar

gdw.  $\Gamma_0 \models A$  für eine endliche Teilmenge  $\Gamma_0 \subseteq \Gamma$  □

Korollar (im Wesentlichen KPS für  $\neg\Gamma$ , HA).

Für eine Formelmenge  $\Gamma$  sind folgende Aussagen äquivalent:

- (a) Jede Belegung erfüllt mindestens eine Formel  $B \in \Gamma$ .
- (b) Es gibt  $n \in \mathbb{N}$  und  $\mathbf{B} \in \Gamma^n$  mit  $B_0 \vee \dots \vee B_{n-1}$  allgemeingültig. □

# Beweis der Hinlänglichkeit für den KPS

Nachfolgend sei  $p_i, i \in \mathbb{N}$ , eine feste Aufzählung von  $\mathcal{A}$ .

## Definition

Eine Formelmenge  $\Gamma$  ist erfüllbar mit Präfix  $\mathbf{b} \in \mathbb{B}^*$ , sofern eine erfüllende Belegung  $\varphi \in \mathbb{B}^{\mathcal{A}}$  mit  $\varphi(p_i) = b_i$  für alle  $i < |\mathbf{b}|$  existiert.

## Proposition

Wenn jede endliche Teilmenge von  $\Gamma$  mit Präfix  $\mathbf{b} \in \mathbb{B}^*$  erfüllbar ist, dann auch mit Präfix  $\mathbf{b}0$  oder  $\mathbf{b}1$ .

## Beweis.

**Annahme:** Es gibt endlichen Teilmengen  $\Gamma_i \subseteq \Gamma$ , die nicht mit Präfix  $\mathbf{b}i$  erfüllbar sind,  $i < 2$ .

Dann ist  $\Gamma_0 \cup \Gamma_1$  nicht mit Präfix  $\mathbf{b}$  erfüllbar, Widerspruch. □

## Beweis (KPS, Hinlänglichkeit).

$\mathcal{A}$  sei abzählbar<sup>a</sup> unendlich und  $\Gamma$  endlich erfüllbar.

**Behauptung:** Es existiert eine Folge  $b_i \in \mathbb{B}$ ,  $i \in \mathbb{N}$ , so dass  $\Gamma$  für jedes  $n \in \mathbb{N}$  endlich mit Präfix  $\langle b_i : i < n \rangle$  erfüllbar ist.

Die Auswahl der  $b_i$  erfolgt induktiv durch Anwendung obiger Proposition, wobei der Induktionsanfang aufgrund der endlichen Erfüllbarkeit von  $\Gamma$  funktioniert (Präfix  $\mathbf{b} = \varepsilon$ ).

**Behauptung:** Die Belegung  $\beta$  mit  $\beta(p_i) = b_i$  erfüllt  $\Gamma$ .

Jede Formel  $A \in \Gamma$  hat einen minimalen Atom-Index  $m$ , so dass aus dem Vorkommen von  $p_i$  in  $A$  folgt  $i < m$ . Folglich wird  $A$  mit Präfix  $\langle b_i : i < m \rangle$  erfüllt. □

---

<sup>a</sup> Im überabzählbaren Fall braucht man eine [transfinite](#) Konstruktion für  $\beta$ .

# Die kanonische Quasiordnung auf $\mathcal{F}[\mathcal{A}]$

Definition (vergl. letztes Beispiel auf ▶ Folie 28)

Für jede Belegung  $\varphi \in \mathbb{B}^{\mathcal{A}}$  induziert  $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$  eine Quasiordnung  $\sqsubseteq_{\varphi}$  auf  $\mathcal{F}[\mathcal{A}]$ ;  $\sqsubseteq^a$  bezeichnet deren Durchschnitt (nicht anti-symm., HA).

<sup>a</sup> Meist wird leider  $\models$  verwendet, ein ohnehin viel zu überladenes Symbol.

## Lemma

Die folgenden Aussagen sind äquivalent für  $A, B \in \mathcal{F}[\mathcal{A}]$ :

- |                     |  |
|---------------------|--|
| ① $B \sqsubseteq A$ | ③ $\{B\}^{\triangleright} \subseteq \{A\}^{\triangleright}$                            |
| ② $\{B\} \models A$ | ④ $\hat{\varphi}(B \rightarrow A) = 1$ für alle $\varphi \in \mathbb{B}^{\mathcal{A}}$ |

Daher kann man  $\sqsubseteq$  als **Externalisierung** des Junktors  $\rightarrow$  auffassen.

**Achtung:** zwar gilt  $\{p, q\} \models p \wedge q$ , aber weder  $p \sqsubseteq p \wedge q$  noch  $q \sqsubseteq p \wedge q$ .

# Die Monotonie der logischen Operationen auf $\mathcal{F}[A]$

## Satz

Die logischen Operationen sind monoton als Abbildungen

$$\mathcal{F}[A]^{\text{op}} \xrightarrow{\neg} \mathcal{F}[A] , \mathcal{F}[A] \times \mathcal{F}[A] \xrightarrow{\star} \mathcal{F}[A] , \mathcal{F}[A]^{\text{op}} \times \mathcal{F}[A] \xrightarrow{\rightarrow} \mathcal{F}[A]$$

(mit  $\star \in \{\wedge, \vee\}$  aber  $\star \neq \leftrightarrow$ ) zwischen quasigeordneten Mengen.

## Beweis

Die kanonischen Interpretationen der Junktoren aus  $\mathcal{J} - \{\leftrightarrow\}$

$$\mathbb{B}^{\text{op}} \xrightarrow{\neg} \mathbb{B} , \mathbb{B} \times \mathbb{B} \xrightarrow{\star} \mathbb{B} , \mathbb{B}^{\text{op}} \times \mathbb{B} \xrightarrow{\rightarrow} \mathbb{B}$$

sind offenbar monoton bzgl.  $\leq$  (warum funktioniert das nicht für  $\leftrightarrow$ ?).

Für jedes  $\varphi \in \mathbb{B}^A$  ist  $\mathcal{F}[A] \xrightarrow{\hat{\varphi}} \mathbb{B}$  per Definition nicht nur ein  $\mathcal{J}$ -Homomorphismus, sondern nach Konstruktion auch monoton bzgl.  $\sqsubseteq_{\varphi}$  und damit bzgl. des Durchschnitts  $\sqsubseteq$  aller  $\sqsubseteq_{\psi}$ ,  $\psi \in \mathbb{B}^A$ . Damit liefern die Junktoren aus  $\mathcal{J} - \{\leftrightarrow\}$  folgende kommutativen Diagramme:

## Fortsetzung

$$\begin{array}{ccccc}
 \mathcal{F}[A]^{\text{op}} & \xrightarrow{\neg} & \mathcal{F}[A] & & \mathcal{F}[A] \times \mathcal{F}[A] & \xrightarrow{\star} & \mathcal{F}[A] & & \mathcal{F}[A]^{\text{op}} \times \mathcal{F}[A] & \xrightarrow{\rightarrow} & \mathcal{F}[A] \\
 \downarrow \hat{\varphi}^{\text{op}} & & \downarrow \hat{\varphi} & , & \downarrow \hat{\varphi} \times \hat{\varphi} & & \downarrow \hat{\varphi} & , & \downarrow \hat{\varphi}^{\text{op}} \times \hat{\varphi} & & \downarrow \hat{\varphi} \\
 \mathbb{B}^{\text{op}} & \xrightarrow{\neg} & \mathbb{B} & & \mathbb{B} \times \mathbb{B} & \xrightarrow{\star} & \mathbb{B} & & \mathbb{B}^{\text{op}} \times \mathbb{B} & \xrightarrow{\rightarrow} & \mathbb{B}
 \end{array}$$

Wäre eine der log. Op'n auf  $\mathcal{F}[A]$  **nicht monoton**, so existierten

- (0)  $A \sqsubseteq B \in \mathcal{F}[A]$  und  $\varphi_0 \in \mathbb{B}^A$  mit  $\hat{\varphi}_0(B) < \hat{\varphi}_0(A)$ ; oder
- (1)  $A \sqsubseteq B, C \sqsubseteq D \in \mathcal{F}[A]$  und  $\varphi_1 \in \mathbb{B}^A$  mit  $\hat{\varphi}_1(B \star D) < \hat{\varphi}_1(A \star C)$ ; oder
- (2)  $A \sqsubseteq B, C \sqsubseteq D \in \mathcal{F}[A]$  und  $\varphi_2 \in \mathbb{B}^A$  mit  $\hat{\varphi}_2(A \rightarrow D) < \hat{\varphi}_2(B \rightarrow C)$

im Widerspruch zu der Tatsache, dass die andere Komposition via  $\mathbb{B}^{\text{op}}$ ,  $\mathbb{B} \times \mathbb{B}$  bzw.  $\mathbb{B}^{\text{op}} \times \mathbb{B}$  nach Konstruktion monoton ist. Folglich sind die obigen logischen Operationen auf  $\mathcal{F}[A]$  ebenfalls monoton. □

Im Folgenden wichtiger als die zugegebenermaßen recht seltsame Quasiordnung  $\sqsubseteq$  auf  $\mathcal{F}[A]$  ist die daraus resultierende Äquivalenzrelation:

# Die kanonische Kongruenz auf $\mathcal{F}[A]$

## Satz

$\equiv := \subseteq \cap \subseteq^{\text{op}}$  ist eine *Kongruenz*:  $A \equiv B$  und  $C \equiv D$  impliziert  
 $\neg A \equiv \neg B$  und  $A \star C \equiv B \star D$  für  $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

## Beweis.

- ▷  $A \equiv B$  gdw.  $A \subseteq B$  und  $B \subseteq A$  gdw.  $\neg B \subseteq \neg A$  und  $\neg A \subseteq \neg B$   
 gdw.  $\neg A \equiv \neg B$
  - ▷  $A \equiv B$  und  $C \equiv D$  gdw.  $A \subseteq B$ ,  $B \subseteq A$ ,  $C \subseteq D$ ,  $D \subseteq C$   
 gdw.  $A \star C \subseteq B \star D$  und  $B \star D \subseteq A \star C$   
 gdw.  $A \star C \equiv B \star D$  für  $\star \in \{\wedge, \vee, \rightarrow\}$
- Außerdem  $A \leftrightarrow C$  gdw.  $A \rightarrow C$  und  $C \rightarrow A$ , analog für  $B \leftrightarrow D$ .  $\square$

## Satz (HA)

Die Menge  $\mathcal{F}[A]/\equiv$  der Äquivalenzklassen ist kanonisch eine  $\mathcal{J}$ -Algebra.



Künftig interessieren Formeln nur noch *bis auf Äquivalenz*, d.h., modulo  $\equiv$ .

Das Verhalten der kanonischen Interpretation der Junktoren in  $\mathbb{B}$  (Folie 53, Folie 54) liefert leicht nachweisbare **Rechenregeln**:

## Satz (HA)

- ▷  $\neg$  ist *selbstinvers*, d.h.,  $\neg\neg A \equiv A$ .
- ▷  $\wedge$  und  $\vee$  sind
  - *idempotent*, d.h.,  $A \wedge A \equiv A \equiv A \vee A$ .
  - *assoziativ*, d.h.,  $(A \star B) \star C \equiv A \star B \star C$  für  $\star \in \{\wedge, \vee\}$ .
  - *kommutativ*, d.h.,  $A \star B \equiv B \star A$  für  $\star \in \{\wedge, \vee\}$ .
  - mit *neutralem Element*  $\top$  bzw.  $\perp$ , d.h.,  $A \wedge \top \equiv A \equiv A \vee \perp$ .
- ▷  $\perp / \top$  *absorbiert* bzgl.  $\wedge / \vee$ , d.h.,  $A \wedge \perp \equiv \perp$  und  $A \vee \top \equiv \top$ .
- ▷ es gelten die **Absorbtionsregeln**

$$A \wedge (A \vee B) \equiv A \quad \text{und} \quad A \vee (A \wedge B) \equiv A \quad \square$$

# Notationelle Konvention + weitere Rechenregeln

Die Assoziativität von  $\wedge$  und  $\vee$  rechtfertigt folgende Schreibweise:

## Notation

$$\bigwedge_{i<0} A_i := \top, \quad \bigwedge_{i<n+1} A_i := \left( \bigwedge_{i<n} A_i \right) \wedge A_n, \quad \text{und dual mit } \bigvee \text{ und } \perp$$

## Satz (HA)

- ① Es gelten die *De Morgan'schen Regeln*:

$$\neg \bigwedge_{i<n} A_i \equiv \bigvee_{i<n} \neg A_i \quad \text{sowie} \quad \neg \bigvee_{i<n} A_i \equiv \bigwedge_{i<n} \neg A_i$$

- ② Es gelten die *Distributivgesetze*:

$$A \wedge \bigvee_{i<n} B_i \equiv \bigvee_{i<n} (A \wedge B_i) \quad \text{sowie} \quad A \vee \bigwedge_{i<n} B_i \equiv \bigwedge_{i<n} (A \vee B_i)$$

# Funktional vollständige Junktorenmengen

Wie bereits erwähnt gibt es  $2^{2^n}$   $n$ -stellige Boole'sche Funktionen.

Wie die De Morganschen Regeln zeigen, sind die durch  $\mathcal{J}$  spezifizierten Funktionen redundant: neben  $\vee$  können z.B. auch  $\rightarrow$  und  $\leftrightarrow$  eliminiert werden, ohne die Ausdrucksfähigkeit zu mindern.

## Definition

Eine Signatur  $\mathcal{I} \xrightarrow{\bar{a}r} \mathbb{N}$  von Junktoren vorgegebener Semantik (= Wahrheitstabellen) heißt **funktional vollständig**, falls jede Boole'sche Funktion  $\mathbb{B}^n \rightarrow \mathbb{B}$  als  $e_A$  für geeignetes  $A \in \mathbf{Term}(\bar{a}r, \mathcal{A})$  auftritt.

## Satz (HA)

$\mathcal{J}$  ist funktional vollständig.

Ist  $\mathcal{I}$  funktional vollständig, so auch jede Junktor-Menge  $\mathcal{I}'$ , deren Junktoren alle  $\mathcal{I}$ -Junktoren simulieren können.

# Post'scher Vollständigkeitssatz (ohne Beweis)

Für  $\mathcal{A}_0 \subseteq \mathcal{A}$  endlich heißt eine Formel  $A \in \mathcal{F}[\mathcal{A}_0]$

- ▷ **konstant**, falls  $\hat{\varphi}(A)$  für beide konstanten Belegungen  $\varphi \in \mathbb{B}^{\mathcal{A}_0}$  denselben Wert wie  $\varphi$  annimmt;
- ▷ **monoton**, falls  $\hat{\varphi}(A) \leq \hat{\psi}(A)$  für alle Belegungen  $\varphi \leq \psi \in \mathbb{B}^{\mathcal{A}_0}$
- ▷ **affin**, falls für jedes Atom  $p \in \mathcal{O}(A)$  die Werte  $\hat{\varphi}(A)$  und  $\hat{\varphi}(A[p/\neg p])$ 
  - entweder für jedes  $\varphi \in \mathbb{B}^{\mathcal{A}_0}$  komplementär sind;
  - oder für jedes  $\varphi \in \mathbb{B}^{\mathcal{A}_0}$  übereinstimmen ( $p$  heißt **Dummy-Variable**);
- ▷ **selbst-dual**, falls  $\hat{\varphi}(A) = 1 - \hat{\varphi}(A[p/\neg p : p \in \mathcal{O}(A)])$  für alle  $\varphi \in \mathbb{B}^{\mathcal{A}_0}$ .

## Satz (Post'scher Vollständigkeitssatz)

$\mathcal{I} \xrightarrow{\bar{a}r} \mathbb{N}$  ist genau dann funktional vollständig, wenn **Term**( $\bar{a}r, \mathcal{A}$ ) je eine Formel enthält, die eine der obigen Eigenschaften **nicht** hat. □

Insbesondere sind  $\{\neg, \wedge\}$ ,  $\{\neg, \vee\}$  und  $\{\neg, \rightarrow\}$  vollständig (HA).

# Kapitel 4

## Deduktion allgemein

# Wozu Deduktion?

Bisher konnten wir die Erfüllbarkeit einer Formel oder einer Formelmenge nur mit semantischen Mitteln überprüfen. Wegen  $\Gamma \models A$  gdw.  $\Gamma \cup \{\neg A\}$  unerfüllbar schließt das den Nachweis korrekter Schlussfolgerungen mit ein.

Mit wachsender Atom-Zahl nimmt der Aufwand Wahrheitstabellen zu erstellen exponentiell zu, stößt also bald an Grenzen.

Nach hinreichend vielen Beispielen wird man feststellen, dass sich bestimmte korrekte Schlüsse allein anhand der Syntax ihrer Prämissen und der Schlussfolgerung erkennen lassen, und kann so den Aufwand einer semantischen Überprüfung vermeiden.

Auf diese Weise erhält man ein „Kalkül“ zur **Ableitung** von Formeln, auch **deduktives System** genannt. Je nach Vorliebe des Autors oder intendierter Anwendung sind viele verschiedene Varianten möglich.

Idealerweise sollte hier die Ableitungsrelation  $\vdash$  eines deduktiven Systems mit der logische Folgerelation  $\models$  übereinstimmen.

# Schlussregeln und Theoreme

## Definition

Ein **deduktives System**  $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$  ( $\mathcal{K}$  für **Kalkül**) besteht aus

- ▷ einer Menge  $\mathcal{F}$  sog. **Formeln**;
- ▷ einer Menge  $\mathcal{R} \subseteq \mathcal{F}^* \times \mathcal{F}$  sog. **Schlussregeln**, oder kurz **Regeln**.

Alternative Schreibweise für Regeln (mit **Prämissen**  $B_i$  und **Konklusion**  $A$ ):

$$\frac{B_0, B_1, \dots, B_{k-1}}{A} \quad \text{anstatt} \quad \langle B_0, B_1, \dots, B_{k-1}; A \rangle \in \mathcal{R}$$

Die Menge  $\mathbf{Ax}(\mathcal{K}) \subseteq \mathcal{F}$  der **Axiome** besteht aus den Konklusionen von Regeln ohne Prämissen, also mit  $k = 0$ . Ihr **Abschluss unter Anwendung von Regeln** (s.u.) liefert die Menge  $\mathbf{Thm}(\mathcal{K}) \subseteq \mathcal{F}$  der **Theoreme**.

Regeln werden oft in **Schemata** zusammengefasst, die **Formel-Variablen** verwenden und zwecks leichter Referenz mit **kurzen Namen** versehen sind.

## Wie erhält man Theoreme? Lange Beweise

Deduktive Systeme sind auch als **Multigraphen** bekannt, deren **Multikanten** (Regeln) endliche Knoten-Tupel mit einzelnen Knoten (Formeln) verbinden.

Regeln lassen sich nun mittels **Substitution** komponieren:

- ▷ Die Prämissen  $B_i$ ,  $i < k$ , einer anzuwendenden Regel müssen als Konklusionen früherer Regelanwendungen verfügbar sein.
- ▷ Schon erzeugte Konklusionen dürfen wiederverwendet werden.
- ▷ Die Axiome als Startpunkte erlauben Konklusionen „aus dem Nichts“.

Theoreme sind Konklusion einer Komposition von Regeln, die mit dem leeren Wort beginnt. Solche Kompositionen nennen wir **langer Beweis**.

Die Wiederverwendbarkeit von Formeln in Kompositionen verträgt sich nicht mit der Bruch-Notation für Regeln. Erzeugt man aber mehrfach benötigte Formeln auch mehrfach, liefert die Bruch-Notation Baum-artige lange Beweise mit recht übersichtlicher Struktur (s.u.).



## Beispiel (Ein deduktives System für partielle Syntax)

Für die vollständige Junktormenge  $\mathcal{J}_0 = \{\neg, \rightarrow\}$  betrachten wir das Alphabet  $\mathcal{J}_0^0[\mathcal{A}]$ . Das deduktive System  $\mathcal{K}_{\text{syn}} = \langle \mathcal{F}_{\text{syn}}, \mathcal{R}_{\text{syn}} \rangle$  verwendet als Formelmenge ganz  $(\mathcal{J}_0^0[\mathcal{A}])^*$  und als Regelmenge

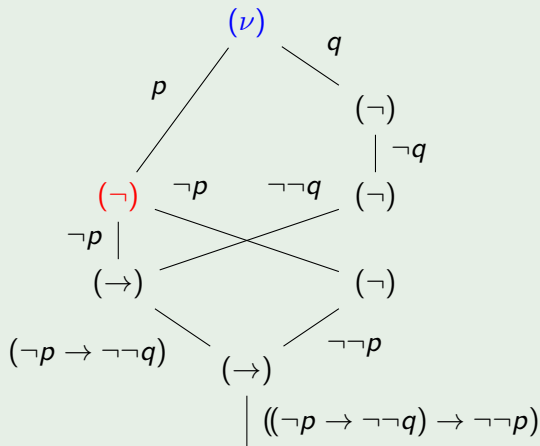
$$\begin{aligned} \mathcal{R}_{\text{syn}} := & \{\varepsilon\} \times \mathcal{A} \cup \{ \langle A, \neg A \rangle : A \in (\mathcal{J}_0^0[\mathcal{A}])^* \} \\ & \cup \{ \langle A, B; (A \rightarrow B) \rangle : A, B \in (\mathcal{J}_0^0[\mathcal{A}])^* \} \end{aligned}$$

oder übersichtlicher in Form von Regelschemata

$$\frac{}{p} \quad (\nu) \quad (p \in \mathcal{A}) \quad , \quad \frac{A}{\neg A} \quad (\neg) \quad \text{und} \quad \frac{A \quad B}{(A \rightarrow B)} \quad (\rightarrow)$$

Die Atome als Axiome liefern die aus dem Syntax-Kapitel bekannten Formeln in den Junktoren  $\neg$  und  $\rightarrow$  als Theoreme.

# Beispiel (Deduktionsgraph für $((\neg p \rightarrow \neg\neg q) \rightarrow \neg\neg p)$ in $\mathcal{K}_{\text{syn}}$ )



Ein Baum benötigt zwei bzw. drei Instanzen von  $(\neg)$  und  $(\nu)$ :

Beispiel (Deduktionsbaum für  $((\neg p \rightarrow \neg\neg q) \rightarrow \neg\neg p)$  in  $\mathcal{K}_{\text{syn}}$ )

$$\frac{\frac{\frac{\overline{p} \quad (\nu)}{\neg p} \quad (\neg)}{(\neg p \rightarrow \neg\neg p)} \quad (\rightarrow)}{\frac{\frac{\overline{q} \quad (\nu)}{\neg q} \quad (\neg)}{\neg\neg q} \quad (\rightarrow)}{((\neg p \rightarrow \neg\neg q) \rightarrow \neg\neg p)} \quad (\rightarrow)}{\frac{\overline{p} \quad (\nu)}{\neg p} \quad (\neg)}{\neg\neg p} \quad (\rightarrow)} \quad (\rightarrow)$$

Beispiel (Ein deduktives System  $\mathcal{K}_{\text{Ar}} = \langle \mathcal{F}_{\text{Ar}}, \mathcal{R}_{\text{Ar}} \rangle$  für die Arithmetik)

Setze  $\mathcal{F}_{\text{Ar}} := \mathbb{Q}$ , die Menge der rationalen Zahlen, und

$$\mathcal{R}_{\text{Ar}} : \quad \frac{}{1} \quad (1) \quad , \quad \frac{x \quad y}{xy} \quad (\times) \quad \text{und} \quad \frac{x \quad y}{x - y} \quad (-) \quad \text{mit} \quad x, y \in \mathbb{Q}$$

Die Theoreme sind genau die ganzen Zahlen. Etwa

$$\frac{\frac{\frac{\overline{1} \quad (1)}{0} \quad (-)}{-1} \quad (-)}{-2} \quad (-) \quad \frac{\overline{1} \quad (1)}{1} \quad (-) \quad \frac{\overline{1} \quad (1)}{1} \quad (-)$$

# Ableitungen und kurze Beweise

**Ziel:** die Redundanz in Deduktionen/langen Beweisen reduzieren:

## Definition

Eine **Ableitung** in  $\mathcal{K} = \langle \mathcal{F}, \mathcal{R} \rangle$  **von**  $A \in \mathcal{F}$  **aus**  $\Gamma \subseteq \mathcal{F}$  ist ein Wort  $\langle A_i : i \leq n \rangle \in \mathcal{F}^{n+1}$  mit  $A_n = A$ , so dass für alle  $k \leq n$  mit  $A_k \notin \Gamma$  gilt

- ▷ es existiert  $\mathbb{N} \ni j \xrightarrow{f} k$  (**Begründung**) mit  $\langle \langle A_{f(i)} : i < j \rangle; A_k \rangle \in \mathcal{R}$ .

$A \in \mathcal{F}$  heißt **aus**  $\Gamma$  **ableitbar**,  $\Gamma \vdash_{\mathcal{K}} A$ , wenn es eine solche Ableitung gibt. Falls  $\Gamma = \emptyset$  spricht man von einem **kurzen Beweis** von  $A$ .

## Satz

*Eine Formel ist genau dann ein Theorem, wenn sie einen kurzen Beweis hat.*

## Beweis.

Induktion über die Länge kurzer Beweise bzw. über die Anzahl der Regeln in langen Beweisen zeigt die Hinlänglich- bzw. Notwendigkeit. (Details: HA)  $\square$

## Beispiel

Ein kurzer Beweis von  $-42$  im obigen deduktiven System  $\mathcal{K}_{Ar}$  ist

$$\langle 1, 0, -1, -2, 4, -6, 36, -42 \rangle$$

Der entsprechende Baum, der  $-42$  im Regelabschluss des Axioms 1 verortet, hat 71 Knoten und der Teilbaum für  $-2$  tritt neunmal darin auf.

Dies zeigt, wieviel Redundanz lange Beweise im Vergleich zu kurzen Beweisen enthalten. Dafür können Ableitungen bzw. kurze Beweise ohne jeglichen Hinweis auf die verwendeten Regeln schwer nachvollziehbar sein.

## Definition

Unter einer **expliziten Ableitung** versteht man eine **vertikale Auflistung** der Folgenglieder mit ihrem Index und ihrer Begründung, samt Namen der verwendeten Regel, bzw. der Angabe "Ann.", falls es sich um ein Element von  $\Gamma$  handelt.

## Beispiel (Expliziter Beweis von $((\neg p \rightarrow \neg\neg q) \rightarrow \neg\neg p)$ in $\mathcal{K}_{\text{syn}}$ )

0.	$p$	$(\nu)$
1.	$\neg p$	$(\neg), 0$
2.	$q$	$(\nu)$
3.	$\neg q$	$(\neg), 2$
4.	$\neg\neg q$	$(\neg), 3$
5.	$(\neg p \rightarrow \neg\neg q)$	$(\rightarrow), 1, 4$
6.	$\neg\neg p$	$(\neg), 1$
7.	$((\neg p \rightarrow \neg\neg q) \rightarrow \neg\neg p)$	$(\rightarrow), 5, 6$

**Achtung:** Die Reihenfolge der Schritte nicht eindeutig. Die doppelte Negation von  $p$  kann z.B. in jeder Position von 2 bis 6 erfolgen.

Je nach Geschmack bzw. gewünschtem Detailgrad kann man lange, kurze und explizite Beweise für Theoreme verwenden.

# Kompaktheit und deduktiver Abschluß

Der Beweis des folgenden Satzes ist viel einfacher als der Beweis seines semantischen Gegenstücks:

## Satz (Kompaktheitssatz, Deduktionsversion (HA))

Eine Formel  $A \in \mathcal{F}$  ist aus  $\Gamma \subseteq \mathcal{F}$  genau dann ableitbar, wenn sie aus einer endlichen Teilmenge  $\Gamma_0 \subseteq \Gamma$  ableitbar ist. □

Eine weiteres zur Semantik analoges Ergebnis hat ebenfalls eine völlig andere Begründung:

## Satz (HA)

Der Abschluß unter  $\vdash_{\mathcal{K}}$  liefert einen Hüllenoperator auf  $\mathbf{P}(\mathcal{F})$ :

$$\Gamma^{\vdash_{\mathcal{K}}} := \{ A \in \mathcal{F} : \Gamma \vdash_{\mathcal{K}} A \}$$

Dessen Fixpunkte nennen wir *deduktiv abgeschlossene Mengen*. □

# Kapitel 5

## Hilbert-Kalkül



# Das Deduktive System $\mathcal{K}_0$

Wir wollen ein deduktives System  $\mathcal{K}_0 = \langle \mathcal{F}_0, \mathcal{R}_0 \rangle$  einführen, für das die Relation  $\vdash_{\mathcal{K}_0}$  mit  $\models$  übereinstimmt. Vereinfachend setzen wir  $\vdash := \vdash_{\mathcal{K}_0}$ .

$\mathcal{F}_0$  besteht aus den Infix-Formeln in  $\mathcal{A}$  über der vollständigen Junktorenmenge  $\mathcal{J}_0 = \{\neg, \rightarrow\}$ , während  $\mathcal{R}_0$  durch vier Schemata gegeben ist (beachte die Klammervereinfachungen!):

$$\triangleright \quad \frac{A \quad A \rightarrow B}{B} \text{ (MP) } \quad \text{Abtrennungsregel oder Modus Ponens}$$

$$\triangleright \quad \frac{}{B \rightarrow A \rightarrow B} \text{ (Ax1)}$$

$$\triangleright \quad \frac{}{(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C} \text{ (Ax2)}$$

$$\triangleright \quad \frac{}{(\neg B \rightarrow \neg A) \rightarrow A \rightarrow B} \text{ (Ax3)}$$

## Lemma

Für jede Formel  $A \in \mathcal{F}_0$  gilt:

$$\vdash A \rightarrow A \quad (\text{Th1})$$

## Beweis.

Wir geben eine explizite Ableitung:

- |    |   |  |
|----|---|--|
| 0. | $A \rightarrow A \rightarrow A$   | Ax1  |
| 1. | $A \rightarrow (A \rightarrow A) \rightarrow A$   | Ax1  |
| 2. | $(A \rightarrow (A \rightarrow A) \rightarrow A) \rightarrow (A \rightarrow A \rightarrow A) \rightarrow A \rightarrow A$ | Ax2  |
| 3. | $(A \rightarrow A \rightarrow A) \rightarrow A \rightarrow A$   | MP, 1,2                                      |
| 4. | $A \rightarrow A$   | MP, 0,3 <span style="float: right;">□</span> |

Achtung: Die Klammerersparnisregeln für  $\rightarrow$  können die Lesbarkeit zunächst beeinträchtigen. Dagegen hilft nur Routine.

# Das syntaktische Deduktionstheorem

Ableitungen in  $\mathcal{K}_0$  können recht umständlich sein. Ein Analogon zum semantischen Deduktionstheorem [▶ Folie 59](#), wird es ermöglichen  $\mathcal{K}_0$ -Ableitungen rekursiv zu verschachteln, was die Effizienz steigert.

Satz (Herbrand, Tarski, veröffentlicht ca. 1930)

$\Gamma \cup \{A\} \vdash B$  genau dann wenn  $\Gamma \vdash A \rightarrow B$ .

Beweis.

( $\Leftarrow$ ) Aus  $\Gamma \cup \{A\}$  lassen sich  $A$  und  $A \rightarrow B$  ableiten, also auch  $B$ .

( $\Rightarrow$ ) Induktion über die Länge einer Ableitung  $\langle B_i : i \leq n \rangle$  für  $\Gamma \cup \{A\} \vdash B = B_n$ . Wir zeigen  $\Gamma \cup \{A\} \vdash B_i$  gdw.  $\Gamma \vdash A \rightarrow B_i$  für  $i \leq n$ .

( $n = 0$ ): Falls  $B_0 = A$ , so gilt nach (Th1)  $\vdash A \rightarrow A$  und somit auch  $\Gamma \vdash A \rightarrow A$ . Andernfalls ist  $B_0$  ein Axiom oder eine Prämisse, und eine Anwendung von (MP) auf  $B_0 \rightarrow A \rightarrow B_0$  (Ax1) liefert  $\Gamma \vdash A \rightarrow B_0$ .

## Beweis, Fortsetzung.

**Annahme:** für jede Ableitung der Länge  $< n$  aus  $\Gamma \cup \{A\}$  und jede Komponente  $C$  darin gelte  $\Gamma \vdash A \rightarrow C$ .

**Schluß:** Nun sei  $\langle B_i : i \leq n \rangle$  eine Ableitung minimaler Länge von  $\Gamma \cup \{A\} \vdash B = B_n$ . Nach Voraussetzung gilt  $\Gamma \vdash A \rightarrow B_i$  für  $i < n$ . Aufgrund der Minimalität muß  $B_n$  aus einer Anwendung von (MP) resultieren, etwa für  $B_i$  und  $B_j = B_i \rightarrow B_n$  mit  $i, j < n$ . Mittels der Instanz  $(A \rightarrow B_i \rightarrow B_n) \rightarrow (A \rightarrow B_i) \rightarrow A \rightarrow B_n$  von (Ax2) und zweimaliger Anwendung von (MP) folgt nun  $\Gamma \vdash A \rightarrow B_n$ . □

Man beachte, dass der Beweis (Ax3) nicht benötigt. Insofern gilt das Deduktionstheorem auch für das schwächere System  $\mathcal{K}_0^-$  ohne (Ax3).

Wir erweitern nun den Begriff der expliziten Ableitung indem wir neben Formeln auch verallgemeinerte explizite Ableitungen als Zeileninhalt zulassen. In einem weiteren Schritt werden wir letztere dann **entfalten**.

# Hybride Ableitungen in $\mathcal{K}_0$

## Definition (rekursiv!)

Eine **hybride Ableitung** von  $A \in \mathcal{F}_0$  aus  $\Gamma \subseteq \mathcal{F}_0$  ist eine Liste  $\langle A_i : i \leq n \rangle$  aus Formeln und hybriden Ableitungen endlicher Schachtelungstiefe mit  $A_n = A$ , die folgende Bedingungen erfüllt: für  $k \leq n$  mit  $A_k \notin \Gamma$  gilt

- (0) entweder existiert  $\mathbb{N} \ni j \xrightarrow{f} k$  mit  $\langle \langle A_{f(i)} : i < j \rangle; A_k \rangle \in \mathcal{R}_0$ ;
- (1) oder  $A_k = B \rightarrow C$  und  $A_{k-1}$  ist eine hybride Ableitung von  $C$  aus  $\Gamma + \{B\}$ ;
- (2) oder  $A_k$  ist eine hybride Ableitung von  $C$  aus  $\Gamma + \{B\}$ , und  $A_{k+1} = B \rightarrow C$ .

Bedingungen (1) und (2) entsprechen Anwendungen von (DT) in Zeilen  $k$  bzw.  $k + 1$ .

**Achtung:** Natürlich kann auch Bedingung (0) Zeilen der Form  $B \rightarrow C$  liefern; solche resultieren nicht exklusiv aus Anwendungen von (DT).

## Definition

Eine **explizite hybride Ableitung** ist eine durchnummerierte vertikale Auflistung der Formeln einer **entfalteten** hybriden Ableitung mit Begründungen in Form des Namens der relevanten Regel bzw. “DT” und Angabe der relevanten Zeilennummern, oder “Ann.” bei Elementen aus  $\Gamma$ .

Wir markieren die Formeln einer echten expliziten hybriden Unter-Ableitung links mit einer eckigen Klammer. Sie muss mit einer **neuen Prämisse**  $B$  als Annahme beginnen, und wenn sie mit einer Formel  $C$  endet, muß die Zeile  $B \rightarrow C$  aufgrund des Deduktionstheorems **unmittelbar** folgen.

**Achtung:** Die Begründung einer Formel  $A_j$  aufgrund einer Regel in  $\mathcal{R}_0$  darf nur Zeilen auf derselben Klammer-Ebene wie  $A_j$  oder darüber referenzieren; tiefere Klammer-Ebenen sind unzugänglich (**out-of-scope**).

**Strategie:** Prämissen mittels geeigneter Annahmen soweit wie möglich zerlegen, Axiome oder schon bewiesene Tautologie-Schemata (s.u.) geschickt(!) einsetzen, um die gewünschte Schlußfolgerung zu erhalten.

## Sieben weitere Tautologie-Schemata

## Lemma

$$\vdash \neg\neg A \rightarrow A$$

(Th2)

## Beweis (hybrid!).

0.	$\neg\neg A$	Ann.
1.	$\neg\neg A \rightarrow \neg\neg\neg\neg A \rightarrow \neg\neg A$	Ax1
2.	$\neg\neg\neg\neg A \rightarrow \neg\neg A$	MP, 0,1
3.	$(\neg\neg\neg\neg A \rightarrow \neg\neg A) \rightarrow \neg A \rightarrow \neg\neg\neg\neg A$	Ax3
4.	$\neg A \rightarrow \neg\neg\neg\neg A$	MP, 2,3
5.	$(\neg A \rightarrow \neg\neg\neg\neg A) \rightarrow \neg\neg A \rightarrow A$	Ax3
6.	$\neg\neg A \rightarrow A$	MP, 4,5
7.	$A$	MP, 0,6
8.	$\neg\neg A \rightarrow A$	DT, 0-7



## Lemma

$$(a) \quad \vdash \neg B \rightarrow B \rightarrow A \quad (\text{Th3})$$

$$(b) \quad \vdash B \rightarrow \neg\neg B \quad (\text{Th4})$$

## Beweis

(a)	0.	$\neg B$	Ann.
	1.	$\neg B \rightarrow \neg A \rightarrow \neg B$	Ax1
	2.	$\neg A \rightarrow \neg B$	MP, 0,1
	3.	$(\neg A \rightarrow \neg B) \rightarrow B \rightarrow A$	Ax3
	4.	$B \rightarrow A$	MP, 2,3
	5.	$\neg B \rightarrow B \rightarrow A$	DT, 0-4

(b)	0.	$\neg\neg\neg B \rightarrow \neg B$	Th2
	1.	$(\neg\neg\neg B \rightarrow \neg B) \rightarrow B \rightarrow \neg\neg B$	Ax3
	2.	$B \rightarrow \neg\neg B$	MP, 0,1





## Lemma

$$\vdash (A \rightarrow B) \rightarrow \neg B \rightarrow \neg A$$

(Th5)

## Beweis.

0.	[	$A \rightarrow B$	Ann.
1.	[	$\neg\neg A$	Ann.
2.	[	$\neg\neg A \rightarrow A$	Th2
3.	[	$A$	MP, 1,2
4.	[	$B$	MP, 3,0
5.	[	$B \rightarrow \neg\neg B$	Th4
6.	[	$\neg\neg B$	MP, 4,5
7.	[	$\neg\neg A \rightarrow \neg\neg B$	DT, 2-7
8.	[	$(\neg\neg A \rightarrow \neg\neg B) \rightarrow \neg B \rightarrow \neg A$	Ax3
9.	[	$\neg B \rightarrow \neg A$	MP, 7,8
10.		$(A \rightarrow B) \rightarrow \neg B \rightarrow \neg A$	DT, 0-9



## Lemma

$$\vdash A \rightarrow \neg B \rightarrow \neg(A \rightarrow B) \quad (\text{Th6})$$

## Beweis.

0.	[	$A$	Ann.
1.	[	$A \rightarrow B$	Ann.
2.	[	$B$	MP, 0,1
3.		$(A \rightarrow B) \rightarrow B$	DT, 2-3
4.		$((A \rightarrow B) \rightarrow B) \rightarrow \neg B \rightarrow \neg(A \rightarrow B)$	Th5
5.		$\neg B \rightarrow \neg(A \rightarrow B)$	MP, 3,4
6.		$A \rightarrow \neg B \rightarrow \neg(A \rightarrow B)$	DT, 0-5

□

## Lemma

$$\vdash (A \rightarrow B) \rightarrow (A \rightarrow \neg B) \rightarrow \neg A \quad (\text{Th7})$$

## Beweis von Th7.

0.	$A \rightarrow B$	Ann.
1.	$A \rightarrow \neg B$	Ann.
2.	$A$	Ann.
3.	$B$	MP, 2,0
4.	$\neg B$	MP, 2,1
5.	$\neg B \rightarrow B \rightarrow X$	Th3
6.	$B \rightarrow X$	MP, 4,5
7.	$X = \neg Y$	MP, 3,6
8.	$A \rightarrow X$	DT, 2-7
9.	$(A \rightarrow X) \rightarrow (\neg X \rightarrow \neg A)$	Th5
10.	$\neg X \rightarrow \neg A$	MP, 8,9
11.	$Y$ z.B. $A \rightarrow A$	irgendeine Tautologie z.B. Th1
12.	$Y \rightarrow \neg\neg Y$	Th4
n-4.	$\neg X = \neg\neg Y$	MP, 11,12
n-3.	$\neg A$	MP (n-4),10
n-2.	$(A \rightarrow \neg B) \rightarrow \neg A$	DT, 1-(n-3)
n-1.	$(A \rightarrow B) \rightarrow (A \rightarrow \neg B) \rightarrow \neg A$	DT, 0-(n-2)



## Lemma

$$\vdash (B \rightarrow A) \rightarrow (\neg B \rightarrow A) \rightarrow A$$

(Th8)

## Beweis.

0.	$B \rightarrow A$	Ann.
1.	$(B \rightarrow A) \rightarrow \neg A \rightarrow \neg B$	Th5
2.	$\neg A \rightarrow \neg B$	MP, 0,1
3.	$\neg B \rightarrow A$	Ann.
4.	$(\neg B \rightarrow A) \rightarrow \neg A \rightarrow \neg\neg B$	Th5
5.	$\neg A \rightarrow \neg\neg B$	MP, 3,4
6.	$(\neg A \rightarrow \neg B) \rightarrow (\neg A \rightarrow \neg\neg B) \rightarrow \neg\neg A$	Th7
7.	$(\neg A \rightarrow \neg\neg B) \rightarrow \neg\neg A$	MP, 2,6
8.	$\neg\neg A$	MP, 5,7
9.	$\neg\neg A \rightarrow A$	Th2
10.	$A$	MP, 8,9
11.	$(\neg B \rightarrow A) \rightarrow A$	DT, 3-10
12.	$(B \rightarrow A) \rightarrow (\neg B \rightarrow A) \rightarrow A$	DT, 0-11



# Zusammenfassung

Künftig dürfen wir neben den ursprünglichen Regeln für  $\mathcal{K}_0$  (MP, Ax1, Ax2, Ax3) und dem syntaktischen Deduktionstheorem (DT) auch die Tautologie-Schemata (Th1) – (Th8) in Ableitungen verwenden:

- ▷ (Th1)  $\vdash A \rightarrow A$
- ▷ (Th2)  $\vdash \neg\neg A \rightarrow A$
- ▷ (Th3)  $\vdash \neg B \rightarrow B \rightarrow A$
- ▷ (Th4)  $\vdash B \rightarrow \neg\neg B$
- ▷ (Th5)  $\vdash (A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$
- ▷ (Th6)  $\vdash A \rightarrow \neg B \rightarrow \neg(A \rightarrow B)$
- ▷ (Th7)  $\vdash (A \rightarrow B) \rightarrow (A \rightarrow \neg B) \rightarrow \neg A$
- ▷ (Th8)  $\vdash (B \rightarrow A) \rightarrow (\neg B \rightarrow A) \rightarrow A$

Wir führen noch eine weitere Vereinfachung für  $\mathcal{K}_0$ -Ableitungen ein:

## Definition

Eine Menge  $\Gamma \subseteq \mathcal{F}_0$  heißt **widersprüchlich** oder **inkonsistent**, wenn eine Formel  $B \in \mathcal{F}_0$  mit  $\Gamma \vdash B$  und  $\Gamma \vdash \neg B$  existiert.

Korollar (Inkonsistenzregel, vergl. ▶ Folie 59)

$\Gamma \cup \{A\}$  inkonsistent gdw.  $\Gamma \vdash \neg A$ .

## Beweis.

( $\Rightarrow$ ): Wähle  $B$  mit  $\Gamma \cup \{A\} \vdash B$  und  $\Gamma \cup \{A\} \vdash \neg B$ , nach (DT) also  $\Gamma \vdash A \rightarrow B$  und  $\Gamma \vdash A \rightarrow \neg B$ . Mit (Th7) folgt dann  $\Gamma \vdash \neg A$ .

( $\Leftarrow$ ):  $\Gamma \vdash \neg A$  impliziert  $\Gamma \cup \{A\} \vdash \neg A$ , während  $\Gamma \cup \{A\} \vdash A$  trivial ist.  $\square$

Sobald im aktuellen Kasten mit Annahme  $B$  ein Widerspruch zu einer früheren zugänglichen Zeile auftritt, beende den Kasten mit dem Symbol  $\perp \notin \mathcal{F}_0$  samt Verweis auf den Widerspruch, und schreibe  $\neg B$  mit Begründung (**IK**) in die nächste Zeile. Das kann Ableitungen verkürzen.

Beispiel ( $\vdash \neg(A \rightarrow B) \rightarrow \neg B$ , direkt und mit (IK))

0.	$\neg(A \rightarrow B)$	Ann.
1.	$\neg(A \rightarrow B) \rightarrow B \rightarrow \neg(A \rightarrow B)$	Ax1
2.	$B \rightarrow \neg(A \rightarrow B)$	MP, 0,1
3.	$B \rightarrow A \rightarrow B$	Ax1
4.	$(B \rightarrow A \rightarrow B) \rightarrow (B \rightarrow \neg(A \rightarrow B)) \rightarrow \neg B$	Th7
5.	$(B \rightarrow \neg(A \rightarrow B)) \rightarrow \neg B$	MP, 3,4
6.	$\neg B$	MP, 2,5
7.	$\neg(A \rightarrow B) \rightarrow \neg B$	DT, 0-6

0.	$\neg(A \rightarrow B)$	Ann.
1.	$B$	Ann.
2.	$B \rightarrow A \rightarrow B$	Ax1
3.	$A \rightarrow B$	MP, 1,2
4.	$\perp$	0,3
5.	$\neg B$	IK, 1-4
6.	$\neg(A \rightarrow B) \rightarrow \neg B$	DT, 0-5

# Die Korrektheit und Vollständigkeit von $\mathcal{K}_0$

**Ziel:** die Ableitungsrelation  $\vdash$  stimmt mit der logischen Folgerrelation  $\models$  überein. Das entspricht dem Nachweis zweier Inklusionen:

- ▷  $\vdash \subseteq \models$ , d.h., jede aus  $\Gamma$  ableitbare Formel ist tatsächlich eine logische Folgerung aus  $\Gamma$ ; man nennt dies die **Korrektheit** von  $\vdash$ ;
- ▷  $\vdash \supseteq \models$ , d.h., jede logische Folgerung aus  $\Gamma$  ist auch aus  $\Gamma$  ableitbar; man nennt dies die **Vollständigkeit** von  $\vdash$ .

Zunächst betrachten wir den Fall  $\Gamma = \emptyset$ .

## Satz (0-Korrektheit)

*Jedes Theorem ist eine Tautologie.*

## Beweis.

Jedes Axiom ist eine Tautologie, Modus Ponens erhält Tautologien, und das Deduktionstheorem erlaubt Verschachtelungen zu entfernen. □



# Vorarbeiten zur 0-Vollständigkeit von $\mathcal{K}_0$

## Satz (0-Vollständigkeit)

*Jede Tautologie ist ein Theorem, d.h., hat einen Beweis.*

Die Anpassung beliebiger Formeln an eine gegebene Belegung erfolgt mit

## Definition

Für  $\varphi \in \mathbb{B}^{\mathcal{A}}$  und  $A \in \mathcal{F}[\mathcal{A}]$  setze

$$\varphi A := \begin{cases} A & \text{falls } \hat{\varphi}(A) = 1 \\ \neg A & \text{sonst} \end{cases} \quad \text{sowie} \quad \varphi \Gamma := \{ \varphi A : A \in \Gamma \}$$

## Lemma

*Für eine endliche Teilmenge  $\mathcal{A}_0$  von Atomen, eine Formel  $A \in \mathcal{F}_0[\mathcal{A}_0]$  (in den Junktoren  $\neg$  und  $\rightarrow$ ) und eine Belegung  $\varphi \in \mathbb{B}^{\mathcal{A}}$  gilt  $\varphi \mathcal{A}_0 \vdash \varphi A$ .*

Beweis. (Strukturelle Induktion über  $A$ )

- ▷  $A = p \in \mathcal{A}_0$  impliziert  $\varphi A \in \varphi \mathcal{A}_0$  und somit  $\varphi \mathcal{A}_0 \vdash \varphi A$ .
- ▷  $A = \neg B$  und  $\varphi \mathcal{A}_0 \vdash \varphi B$ : falls  $\hat{\varphi}(B) = 0$ , d.h.  $\varphi(\neg B) = \neg B$ , ist man fertig. Sonst wende (DT) auf  $\varphi \mathcal{A}_0 \vdash B$  und  $\vdash B \rightarrow \neg\neg B$  (Th4) an.
- ▷  $A = B \rightarrow C$  und  $\varphi \mathcal{A}_0 \vdash \varphi B$  sowie  $\varphi \mathcal{A}_0 \vdash \varphi C$ : wende (DT) an, wegen  $\varphi(B \rightarrow C) = B \rightarrow C$  gdw.  $\hat{\varphi}(B) = 0$  oder  $\hat{\varphi}(C) = 1$  auf
  - $\varphi \mathcal{A}_0 \vdash \neg B$  und  $\vdash \neg B \rightarrow B \rightarrow C$  (Th3), falls  $\hat{\varphi}(B) = 0$ ;
  - $\varphi \mathcal{A}_0 \vdash C$  und  $\vdash C \rightarrow B \rightarrow C$  (Ax1), falls  $\hat{\varphi}(C) = 1$ ;
  - $\varphi \mathcal{A}_0 \vdash B$ ,  $\varphi \mathcal{A}_0 \vdash \neg C$  und  $\vdash B \rightarrow \neg C \rightarrow \neg(B \rightarrow C)$  (Th6), sonst.  $\square$

## Lemma

Mit  $\Gamma \cup \{B\} \vdash A$  und  $\Gamma \cup \{\neg B\} \vdash A$  gilt auch  $\Gamma \vdash A$ .

## Beweis.

(DT) liefert  $\Gamma \vdash B \rightarrow A$  sowie  $\Gamma \vdash \neg B \rightarrow A$ . Zweimalige Anwendung von (MP) auf (Th8) liefert das gewünschte Ergebnis.  $\square$

Beweis der 0-Vollständigkeit von  $\mathcal{K}_0$ 

## Beweis.

$A$  sei eine **Tautologie**, in der  $n$  Atome auftreten, etwa  $\{p_i : i < n\}$ .  
 Nach dem ersten Lemma gilt für jede Belegung  $\varphi$

$$\varphi\{p_i : i < n\} \vdash \varphi A = A \quad (\star)$$

Wähle nun  $\varphi$  beliebig und setze für  $k \leq n$

$$\varphi_k(p_i) = \begin{cases} \varphi(p_i) & \text{falls } i < k \\ 1 - \varphi(p_i) & \text{falls } k \leq i < n \end{cases}$$

All diese  $n + 1$  Belegungen erfüllen  $(\star)$ . Da sich  $\varphi_j\{p_i : i < n\}$  und  $\varphi_{j+1}\{p_i : i < n\}$  genau bei  $p_j$  unterscheiden, liefert das zweite Lemma  $\varphi\{p_i : i < k\} \vdash A$  absteigend für alle  $k < n$ , speziell  $\emptyset \vdash A$  für  $k = 0$ .  $\square$

Korrektheit und Vollständigkeit von  $\mathcal{K}_0$ 

## Satz

*A ist genau dann in  $\mathcal{K}_0$  aus  $\Gamma$  ableitbar, wenn A logisch aus  $\Gamma$  folgt.*

## Beweis.

$\Gamma \vdash A$  gdw. es gibt  $\Gamma \supseteq \{B_i : i < n\} \vdash A$

gdw.  $\vdash B_0 \rightarrow B_1 \rightarrow \dots \rightarrow B_{n-1} \rightarrow A$

gdw.  $\models B_0 \rightarrow B_1 \rightarrow \dots \rightarrow B_{n-1} \rightarrow A$

gdw. es gibt  $\Gamma \supseteq \{B_i : i < n\} \models A$

gdw.  $\Gamma \models A$



Hier wurden auf der semantischen und der syntaktischen Seite jeweils die entsprechenden Kompaktheitssätze und Deduktionstheoreme angewendet, und „in der Mitte“ die obige prämissenfreie Variante des Satzes.

# Bemerkungen

- ▷ Der wesentliche Punkt des obigen Beweises ist die Verfügbarkeit des syntaktischen Deduktionstheorems (DT) für den Kalkül  $\mathcal{K}_0$ .
- ▷ Für andere Kalküle  $\mathcal{K}$  mit dem Junktor  $\rightarrow$  stellt sich die Frage, ob sie ein Deduktionstheorem  $\Gamma \vdash_{\mathcal{K}} A \rightarrow B$  gdw.  $\Gamma \cup \{A\} \vdash_{\mathcal{K}} B$  erfüllen.
- ▷ Man kann zeigen, dass dann die Schemata (MP), (Ax1) und (Ax2) ableitbar sind. Das Schema (Ax3), das nicht im Beweis des (DT) für  $\mathcal{K}_0$  verwendet wurde, kann hingegen auch durch andere Schemata ersetzt werden (z.B. Varianten des **Modus Tollens**  $\frac{A \rightarrow B \quad \neg B}{\neg A}$  (MT)).
- ▷ Deduktive Systeme der Logik, die wie  $\mathcal{K}_0$  Axiome aber möglichst wenige Schlussregeln verwenden, werden **Hilbert**<sup>2</sup>-Kalküle genannt.  $\mathcal{K}_0$  selbst geht auf **Łukasiewicz**<sup>3</sup> zurück, und stellt eine Vereinfachung des bahnbrechenden Systems von **Frege**<sup>4</sup> dar.

---

<sup>2</sup> David Hilbert (1862–1943)

<sup>3</sup> Jan Łukasiewicz (1878–1956), auch Erfinder der sog. „polnischen Notation“

<sup>4</sup> Gottlob Frege (1848–1925)

## Nachteile des Hilbert-Kalküls

Die axiomatische Methode des Hilbert-Kalküls  $\mathcal{K}_0$ , mit nur einer Schlussregeln und beschränkter Junktorenmenge, hat einige Nachteile:

- ▶ Das Verfahren ist unhandlich; erst in Verbindung mit dem externen(!) Deduktionstheorem scheint effizientes Arbeiten möglich zu sein.
- ▶ Die herausgehobene Bedeutung des Junktors  $\rightarrow$  und die Auswahl der Axiomschemata gelten nicht universell als Vorteile: was etwa zeichnet (Ax2) aus, wenn  $A \rightarrow A$  aufwändig hergeleitet werden muss?
- ▶ Modus Ponens als einzige Schlussregeln erschwert die mechanische, etwa Computer-gestützte, Suche nach Beweisen, bei der man von der gewünschten Konklusion rückwärts auf geeignete Axiome hinarbeitet, denn Modus Ponens reduziert die Komplexität von Formeln.
- ▶ Zumindest subjektiv spiegeln Beweise in  $\mathcal{K}_0$  die tatsächliche Arbeitsweise von Mathematikern nur sehr eingeschränkt wider; diese untersucht häufig die Konsequenzen bestimmter Annahmen (benötigt (DT)) und verwendet uneingeschränkt Konjunktion wie Disjunktion.

# Kapitel 6

## Natürliche Deduktion und Sequenzen-Kalkül (optional)

# Geschichte und Überblick

1934 erschienen unabhängig voneinander zwei Vorschläge für ein deduktives System  $\mathcal{K}_{\text{nat}}$ , das die tatsächliche mathematische Arbeitsweise besser widerspiegeln sollte: die Arbeiten von Jaśkowski<sup>5</sup> (mit Vorarbeiten seit mindestens 1929) und Gentzen<sup>6</sup> (basierend auf seiner Dissertation von 1933) begründeten den Kalkül des sog. [natürlichen Schließens](#); zu Hintergrund und Einordnung siehe auch [Pelletier-Hazen](#). Auch für Computer-unterstützte Beweissysteme ist  $\mathcal{K}_{\text{nat}}$  (wie auch der noch zu besprechende Sequenzen-Kalkül Gentzens) dem Hilbert-Kalkül  $\mathcal{K}_0$  deutlich überlegen.

Während Gentzen für Ableitungen zur [Baumnotation](#) griff, nutzte Jaśkowski bereits eine vertikale Auflistung mit Blockstruktur (Kästen statt linker Klammern), verwendete später aber die Zeilenlabel zur Buchführung.

---

<sup>5</sup> Stanisław Jaśkowski (1906–1965): On the rules of suppositions in formal logic, *Studia Logica* 1, 5–32, 1934

<sup>6</sup> Gerhard Gentzen (1909–1945): Untersuchungen über das logische Schließen. I, *Mathematische Zeitschrift*, 39(2), 176–210, 1934



# Grundlagen

- ▷  $\mathcal{F}_{\text{nat}}$  enthält alle Formeln in  $\mathcal{A}$  über  $\mathcal{J}_{\text{nat}} = \{\perp, \neg, \wedge, \vee, \rightarrow\}$ .
- ▷  $\mathcal{K}_{\text{nat}}$  hat keine Axiome,  $\mathcal{R}_{\text{nat}}^-$  enthält 11 Schemata, und zwar Einführungs- und Eliminationsregeln für  $\neg$ ,  $\wedge$ ,  $\vee$ , und  $\rightarrow$ , sowie eine Eliminationsregel für  $\perp$ . Dies deckt bereits die **konstruktivistische** oder **intuitionistische** Logik ab. Hinzufügen von (DNE) “double negation elimination”, oder (LEM) (“law of excluded middle”), oder (PBC) (“proof by contradiction”) liefert  $\mathcal{K}_{\text{nat}}$  für **klassische** Logik. Wir schreiben  $\vdash$  statt  $\vdash_{\text{nat}}$  (zur Unterscheidung von  $\vdash$ ).
- ▷ **Achtung:** In Ableitungen **kann** jeder Einführungsregel eine entsprechende Eliminationsregel folgen, sofern deren **Hauptteile** (unten rot markiert) übereinstimmen (nicht zielführende Macke des Kalküls).
- ▷ Drei der Regeln entfalten eine **Fernwirkung**:  $(\rightarrow i)$  simuliert das Deduktionstheorem in den hybriden Ableitungen des Hilbert-Kalküls direkt, und  $(\neg i)$  entspricht dem Korollar zum **(sDT)**. Dagegen hat  $(\vee e)$  kein Vorbild in  $\mathcal{R}_0$  und bedarf einer separaten Überlegung.

## Die Regeln für Konjunktion und Implikation

	Introduktion	Elimination
$\wedge$	$\frac{G \quad H}{G \wedge H} (\wedge i)$	$\frac{G \wedge H}{G} (\wedge e) \quad \text{sowie} \quad \frac{G \wedge H}{H} (\wedge e)$
$\rightarrow$	$\frac{\begin{array}{c} [G \\ \vdots \\ H \end{array}}{G \rightarrow H} (\rightarrow i)$	$\frac{G \quad G \rightarrow H}{H} (\rightarrow e)$

- ▷  $(\rightarrow e)$  entspricht Modus Ponens (MP) aus dem Hilbert-Kalkül  $\mathcal{K}_0$ .
- ▷  $(\rightarrow i)$  ist ein neuer Typ von Regel, die es ermöglichen soll, den Effekt von DT in hybriden  $\mathcal{K}_0$ -Ableitungen in  $\mathcal{K}_{\text{nat}}$  direkt zu realisieren. Sie erlaubt, eine Teildableitung von  $H$  aus der um  $G$  vergrößerten aktuellen Prämissenmenge zugunsten von  $G \rightarrow H$  unzugänglich zu machen.

# Die Regeln für Disjunktion, Negation und Absurdität

	Introduktion	Elimination
$\vee$	$\frac{G}{G \vee H} (\vee i)$ sowie $\frac{H}{G \vee H} (\vee i)$	$\frac{G \vee H \quad \left[ \begin{array}{c} G \\ \vdots \\ K \end{array} \right] \quad \left[ \begin{array}{c} H \\ \vdots \\ K \end{array} \right]}{K} (\vee e)$
$\neg$	$\frac{\left[ \begin{array}{c} G \\ \vdots \\ \perp \end{array} \right]}{\neg G} (\neg i)$	$\frac{G \quad \neg G}{\perp} (\neg e)$
$\perp$	$\frac{}{\neg \perp} (\perp i)$ ableitbar! (HA)	$\frac{\perp}{G} (\perp e)$
$\neg\neg$	$\frac{G}{\neg\neg G} (\text{DNI})$ ableitbar! (HA)	$\frac{\neg\neg G}{G} (\text{DNE})$

- ▷  $(\neg i)$  entspricht (IK) und kann wegen  $(\rightarrow i)$  ersetzt werden durch

$$\frac{G \rightarrow \perp}{\neg G}$$

was Ableitungen an dieser Stelle um eine Zeile verlängert.

- ▷ Die Regel  $(\vee e)$  ist am kompliziertesten anzuwenden: kann  $G \vee H$  aus den aktuellen Prämissen abgeleitet werden, sind zwei Teildableitungen von  $K$  aus der um  $G$  bzw.  $H$  vergrößerten Prämisenmenge einzuschachteln, zugunsten von  $K$ .
- ▷ Alle Regeln entsprechen wahren semantischen Sachverhalten bzw. korrekten logischen Folgerungen, damit sollte  $\mathcal{K}_{\text{nat}}$  korrekt sein (s.u.).

## Definition

**Explizite Ableitungen** sind nun vertikale nummerierte Auflistungen von Formeln mit Blockstruktur (linke eckige Klammern), deren Begründungen gemäß der Regeln auf vorangehende Formeln bzw. Blöcke verweisen. Auf einzelne Formeln in Blöcken kann von außerhalb nicht verwiesen werden.

## Satz

$$\vdash F \vee \neg F$$

## Beweis

0.	[	$\neg(F \vee \neg F)$	Ann.
1.	[	$F$	Ann.
2.	[	$F \vee \neg F$	$(\vee i), 1$
3.	[	$\perp$	$(\neg e), 0,2$
4.	[	$\neg F$	$(\neg i), 1-3$
5.	[	$F \vee \neg F$	$(\vee i), 4$
6.	[	$\perp$	$(\neg e), 0,5$
7.	[	$\neg\neg(F \vee \neg F)$	$(\neg i), 0-6$
8.		$F \vee \neg F$	$(DNE), 7$



## Beispiel (oberer Beweis als Baum)

$$\begin{array}{c}
 \frac{\frac{[F]}{F \vee \neg F} (\vee i)}{[\neg(F \vee \neg F)]} (\neg e) \\
 \frac{\perp}{\neg F} (\neg i) \\
 \frac{F \vee \neg F}{(\neg e)} \\
 \frac{[\neg(F \vee \neg F)]}{(\neg e)} \\
 \frac{\perp}{\neg\neg(F \vee \neg F)} (\neg i) \\
 \frac{\neg\neg(F \vee \neg F)}{F \vee \neg F} (\text{DNE})
 \end{array}$$

Der Gültigkeitsbereich (Scope) der jeweiligen geschachtelten Teilab-  
 leitungen ist nur schwer auszumachen. Trotz der farblichen Markierung des  
 jeweiligen Anfangs und Endes ist nicht offensichtlich, dass die „blaue  
 Schachtel“ innerhalb der „roten Schachtel“ liegt.

In dieser VL werden wir die Baum-Darstellung erst bei Gentzens  
 Sequenzen-Kalkül wieder aufgreifen.

## Satz

In  $\mathcal{K}_{\text{nat}}$  lässt sich (DNE) äquivalent ersetzen durch

$$\overline{F \vee \neg F} \quad (\text{LEM})$$

## Beweis

Es genügt, im neuen Kalkül  $\neg\neg F \vdash F$  nachzuweisen.

0.	$\neg\neg F$	Prämisse
1.	[ $\neg F$	Ann.
2.	$\perp$	$(\neg e)$ , 0,1
3.	$F$	$(\perp e)$ , 3
4.	[ $F$	Ann.
5.	$F \vee \neg F$	LEM
6.	$F$	$(\vee e)$ , 5, 1-3, 4-4



## Satz

$\Gamma \cup \{\neg G\} \vdash \perp$  gdw  $\Gamma \vdash \neg\neg G$  (immer) gdw  $\Gamma \vdash G$  (klassisch).

## Beweis.

( $\Rightarrow$ ) Falls  $\Gamma \vdash \perp$ , wende ( $\perp e$ ) an. Andernfalls gibt es eine Ableitung für  $\perp$  aus  $\Gamma \cup \{\neg G\}$  mit erster Zeile  $\neg G$ . Anwendung von ( $\neg i$ ) liefert  $\Gamma \vdash \neg\neg G$ , und mit (DNE) folgt  $\Gamma \vdash G$ .

( $\Leftarrow$ ) Wende ( $\neg e$ ) auf  $\Gamma \cup \{\neg G\} \vdash G$  bzw.  $\Gamma \cup \{\neg G\} \vdash \neg\neg G$  an. □

## Satz (HA)

In  $\mathcal{K}_{\text{nat}}$  lässt sich (DNE) äquivalent ersetzen durch

$$\frac{\left[ \begin{array}{c} \neg G \\ \vdots \\ \perp \end{array} \right]}{G} \text{ (PBC)}$$



## „Normalformen“ und die Teilformel-Eigenschaft

Einer Introduction die entsprechende Elimination folgen zu lassen, so dass die Hauptteile (rot markiert) übereinstimmen, verlängert einen Beweis unnötig ohne Fortschritt.

Im Kalkül  $\mathcal{K}_{\text{nat}}^-$  ohne die Regel (DNE) hat das folgenden positiven Effekt:

### Satz

*In  $\mathcal{K}_{\text{nat}}^-$  lässt sich jeder Beweis durch Eliminierung der oben genannten Introduktions-Eliminations-Paare in eine „Normalform“ mit der sog. **Teilformel-Eigenschaft** bringen: jede auftretende Formel ist Teilformel der Konklusion oder einer der Prämissen/Annahmen.* □

Man zerlegt einfach alle Prämissen durch Eliminationsregeln, und die gewünschte Konklusion rückwärts durch Introduktionsregeln, bis Übereinstimmung eintritt, oder nicht. Leider lassen sich in der klassischen Logik mit (DNE) (oder (LEM) oder (PBC)) Beweise nicht so einfach finden.

# Ausdrucksstärke im Vergleich zum Hilbert-Kalkül

## Satz

Die Axiom-Schemata (Ax1), (Ax2) und (Ax3) des Hilbert-Kalküls sind Theoreme in  $\mathcal{K}_{\text{nat}}$ .

## Beweis

(Ax1):

0.	[	$B$	Ann.
1.	[	$A$	Ann.
2.	[	$A \wedge B$	$(\wedge i), 1,0$
3.	[	$B$	$(\wedge e), 2$
4.	[	$A \rightarrow B$	$(\rightarrow i), 1-3$
5.		$B \rightarrow A \rightarrow B$	$(\rightarrow i), 0-4$

## Beweis (Fortsetzung)

(Ax2):

0.	[	$A \rightarrow B \rightarrow C$	Ann.
1.	[	$A \rightarrow B$	Ann.
2.	[	$A$	Ann.
3.	[	$B$	$(\rightarrow e)$ , 2,1
4.	[	$B \rightarrow C$	$(\rightarrow e)$ , 2,0
5.	[	$C$	$(\rightarrow e)$ , 3,4
6.	[	$A \rightarrow C$	$(\rightarrow i)$ , 2-5
7.	[	$(A \rightarrow B) \rightarrow A \rightarrow C$	$(\rightarrow i)$ , 1-6
8.		$(A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow B) \rightarrow A \rightarrow C$	$(\rightarrow i)$ , 0-7

## Beweis (Fortsetzung)

(Ax3):

0.	$\neg B \rightarrow \neg A$	Ann.
1.	$A$	Ann.
2.	$\neg B$	Ann.
3.	$\neg A$	$(\rightarrow e)$ , 2,0
4.	$\perp$	$(\neg e)$ , 1,3
5.	$\neg\neg B$	$(\neg i)$ , 2-4
6.	$B$	$(DNE)$ , 5
7.	$A \rightarrow B$	$(\rightarrow i)$ , 1-6
8.	$(\neg B \rightarrow \neg A) \rightarrow A \rightarrow B$	$(\rightarrow i)$ , 0-7



## Korollar

Die Theoreme (Th1)–(Th8) des Hilbert-Kalküls sind Theoreme in  $\mathcal{K}_{\text{nat}}$ .  $\square$

# Einige Hilfssätze

Die obigen Theoreme liefern einige nützliche Rechenregeln:

## Korollar

- ▷  $\neg B \vdash B \rightarrow A$  (tH3)
- ▷  $B \vdash \neg\neg B$  (tH4)
- ▷  $A \rightarrow B \vdash \neg B \rightarrow \neg A$  (tH5)
- ▷  $A, \neg B \vdash \neg(A \rightarrow B)$  (tH6)
- ▷  $A \rightarrow B, A \rightarrow \neg B \vdash \neg A$  (tH7)
- ▷  $B \rightarrow A, \neg B \rightarrow A \vdash A$  (tH8)

(tH4) lässt sich aber schneller direkt zeigen als via  $\mathcal{K}_0$ , HA!

Künftig werden wir diese abgeleiteten Regeln wie auch (LEM) und (PBC) zur Verkürzung von Beweisen einsetzen.

## Lemma (Contraposition)

$$F \rightarrow G \vdash \neg G \rightarrow \neg F \text{ und } \neg G \rightarrow \neg F \vdash F \rightarrow G. \quad (\text{CP})+(\text{PC})$$

## Beweis.

0.	$F \rightarrow G$	Prämisse
1.	$\neg G$	Ann.
2.	$F$	Ann.
3.	$G$	$(\rightarrow e), 2,0$
4.	$\perp$	$(\neg e), 3,1$
5.	$\neg F$	$(\neg i), 2-4$
6.	$\neg F \rightarrow \neg G$	$(\rightarrow i), 1-5$

0.	$\neg G \rightarrow \neg F$	Prämisse
1.	$F$	Ann.
2.	$\neg G$	Ann.
3.	$\neg F$	$(\rightarrow e), 1,0$
4.	$\perp$	$(\neg e), 3,1$
5.	$G$	$(\text{PBC}), 2-4$
6.	$F \rightarrow G$	$(\rightarrow i), 1-5$



(CP) ist zwar schon als (tH5) bekannt, aber dieser  $\mathcal{K}_{\text{nat}}$ -Beweis ist kürzer als der obige [Beweis](#) in  $\mathcal{K}_0$ .

## Lemma (1. De Morgansche Regel)

$\neg(G \vee H) \vdash \neg G \wedge \neg H$  und  $\neg G \wedge \neg H \vdash \neg(G \vee H)$ . (DM1)

### Beweis.

0.	$\neg(G \vee H)$	Prämisse
1.	[ $G$	Ann.
2.	$G \vee H$	$(\vee i)$ , 1
3.	$\perp$	$(\neg e)$ , 2,0
4.	$\neg G$	$(\neg i)$ , 1-3
5.	[ $H$	Ann.
6.	$G \vee H$	$(\vee i)$ , 5
7.	$\perp$	$(\neg e)$ , 7,0
8.	$\neg H$	$(\neg i)$ , 5-7
9.	$\neg G \wedge \neg H$	$(\wedge i)$ , 4,8

0.	$\neg G \wedge \neg H$	Prämisse
1.	[ $G \vee H$	Ann.
2.	[ $G$	Ann.
3.	$\neg G$	$(\wedge e)$ , 0
4.	$\perp$	$(\neg e)$ , 2,3
5.	[ $H$	Ann.
6.	$\neg H$	$(\wedge e)$ , 0
7.	$\perp$	$(\neg e)$ , 5,6
8.	$\perp$	$(\vee e)$ , 1,2-4,5-7
9.	$\neg(G \vee H)$	$(\neg i)$ , 1-8



## Lemma (2. De Morgansche Regel)

$\neg G \vee \neg H \vdash \neg(G \wedge H)$  und  $\neg(G \wedge H) \vdash \neg G \vee \neg H$ .

(DM2)

### Beweis.

0.	$\neg G \vee \neg H$	Prämisse
1.	[ $G \wedge H$	Ann.
2.	$G$	( $\wedge e$ ), 1
3.	$H$	( $\wedge e$ ), 1
4.	$\neg\neg G$	(tH4), 2
5.	$\neg\neg H$	(tH4), 3
6.	$\neg\neg G \wedge \neg\neg H$	( $\wedge i$ ), 5,6
7.	$\neg(\neg G \vee \neg H)$	DM1, 7
8.	$\perp$	( $\neg e$ ), 0,8
9.	$\neg(G \wedge H)$	( $\neg i$ ), 1-9

0.	$\neg(G \wedge H)$	Prämisse
1.	[ $\neg(\neg G \vee \neg H)$	Ann.
2.	$\neg\neg G \wedge \neg\neg H$	DM1
3.	$\neg\neg G$	( $\wedge e$ ), 2
4.	$\neg\neg H$	( $\wedge e$ ), 2
5.	$G$	(DNE), 3
6.	$H$	(DNE), 4
7.	$G \wedge H$	( $\wedge i$ ), 5,6
8.	$\perp$	( $\neg e$ ), 7,0
9.	$\neg G \vee \neg H$	(PBC), 1-8





## Lemma (Ersetzung der Junktoren $\vee$ und $\wedge$ )

$G \vee H \vdash \neg G \rightarrow H$  und  $G \wedge H \vdash \neg(H \rightarrow \neg G)$ .

$(\vee x) + (\wedge x)$

### Beweis.

0.	$G \vee H$	Prämisse
1.	[ $G$	Ann.
2.	[ [ $\neg G$	Ann.
3.	[ [ $\perp$	$(\neg e), 1,2$
4.	[ [ $H$	$(\perp e), 3$
5.	[ $\neg G \rightarrow H$	$(\rightarrow i), 2-4$
6.	[ $H$	Ann.
7.	[ [ $\neg G$	Ann.
8.	[ [ $\neg G \wedge H$	$(\wedge i), 7,6$
9.	[ [ $H$	$(\wedge e), 8$
10.	[ $\neg G \rightarrow H$	$(\rightarrow i), 7-9$
11.	$\neg G \rightarrow H$	$(\vee e), 0,1-5,6-10$

0.	$G \wedge H$	Prämisse
1.	$G$	$(\wedge e), 0$
2.	$H$	$(\wedge e), 0$
3.	[ $H \rightarrow \neg G$	Ann.
4.	[ [ $\neg G$	$(\rightarrow e), 2,3$
5.	[ [ $\perp$	$(\neg e), 1,4$
6.	$\neg(H \rightarrow \neg G)$	$(\neg i), 3-5$



Lemma (Rückersetzung der Junktoren  $\vee$  und  $\wedge$ )

$$\neg G \rightarrow H \vdash G \vee H \text{ und } \neg(H \rightarrow \neg G) \vdash G \wedge H \quad (\forall z) + (\wedge z)$$

## Beweis.

0.	$\neg G \rightarrow H$	Prämisse		0.	$\neg(H \rightarrow \neg G)$	Prämisse
1.	$\neg H \rightarrow \neg\neg G$	(CP), 0		1.	$\neg(G \wedge H)$	Ann.
2.	$\neg(F \vee G)$	Ann.		2.	$\neg G \vee \neg H$	DM1, 1
3.	$\neg G \wedge \neg H$	DM2, 2		3.	$\neg\neg G \rightarrow \neg H$	( $\vee x$ ), 1,0
4.	$\neg(\neg H \rightarrow \neg\neg G)$	( $\vee x$ ), 3		4.	$H \rightarrow \neg G$	(CP), 3
5.	$\perp$	( $\neg e$ ), 1,4		5.	$\perp$	( $\neg e$ ), 0,4
6.	$G \vee H$	(PBC), 2–5		6.	$F \wedge G$	(PBC), 1–5



Der Junktor  $\perp$  kann durch  $\neg(p \rightarrow p)$  mit einem frischen Atom  $p$  ersetzt werden. Wir sind nun in der Lage,  $\mathcal{K}_{\text{nat}}$  mit  $\mathcal{K}_0$  in Beziehung zu setzen.

Die Vollständigkeit von  $\mathcal{K}_{\text{nat}}$ 

## Satz

Jede Tautologie ist ein  $\mathcal{K}_{\text{nat}}$ -Theorem, d.h.,  $\mathcal{K}_{\text{nat}}$  ist 0-vollständig.

## Beweis.

Jede Tautologie  $F$  bzgl.  $\mathcal{J}_{\text{nat}} = \{\neg, \rightarrow, \wedge, \vee, \perp\}$  kann mittels  $G \vee H \equiv \neg G \rightarrow H$  und  $G \wedge H \equiv \neg(H \rightarrow \neg G)$  sowie  $\perp \equiv \neg(p \rightarrow p)$  in eine Tautologie  $F'$  bzgl.  $\mathcal{J}_0 = \{\neg, \rightarrow\}$  transformiert werden. Diese ist ein  $\mathcal{K}_0$ -Theorem, im Hinblick auf die  $\mathcal{K}_0$ -Axiome also auch ein  $\mathcal{K}_{\text{nat}}$ -Theorem. Aufgrund von  $\neg G \rightarrow H \vdash G \vee H$  und  $\neg(H \rightarrow \neg G) \vdash G \wedge H$  sowie  $\neg(p \rightarrow p) \vdash \perp$  lassen sich die obigen Transformationsschritte in  $\mathcal{K}_{\text{nat}}$  rückgängig machen. Damit ist  $F$  ebenfalls ein  $\mathcal{K}_{\text{nat}}$ -Theorem.  $\square$

► Folie 133

Auch ein direkter Beweis ohne Rückgriff auf das  $\mathcal{K}_0$ -Ergebnis ist möglich. Dazu sind die vorbereitenden Lemmata [► Lemma](#) und [► Lemma](#) anzupassen.

## Lemma

Für eine Teilmenge  $\mathcal{A}_0$  von Atomen, eine Formel  $A \in \mathcal{F}_{\text{nat}}[\mathcal{A}_0]$  über  $\mathcal{J}_{\text{nat}}$  und eine Belegung  $\varphi \in \mathbb{B}^{\mathcal{A}}$  gilt  $\varphi \mathcal{A}_0 \vdash \varphi A$ .

Beweis. (Strukturelle Induktion über  $A$ )

- ▷  $A = \perp$  trivial wegen  $(\perp i)$ .
  - ▷  $A = p \in \mathcal{A}_0$  impliziert  $\varphi A \in \varphi \mathcal{A}_0$ .
  - ▷  $A = \neg B$  und  $\varphi \mathcal{A}_0 \vdash \varphi B$ :  $\varphi(\neg B) = \neg B$  gdw.  $\hat{\varphi}(B) = 0$ .  
Z.z.  $\neg B \vdash \neg B$  (trivial) und  $B \vdash \neg\neg B$  (umseitig).
  - ▷  $A = B \star C$  und  $\varphi \mathcal{A}_0 \vdash \varphi B$  sowie  $\varphi \mathcal{A}_0 \vdash \varphi C$ .
    - $\varphi(B \wedge C) = B \wedge C$  gdw.  $\hat{\varphi}(B) = 1 = \hat{\varphi}(C)$ .  
Z.z.  $\{B, C\} \vdash B \wedge C$  sowie  $\neg B \vdash \neg(B \wedge C)$  und  $\neg C \vdash \neg(B \wedge C)$ .
    - $\varphi(B \vee C) = B \vee C$  gdw.  $\hat{\varphi}(B) = 1 = 1$  oder  $\hat{\varphi}(C) = 1$ .  
Z.z.  $B \vdash B \vee C$  und  $C \vdash B \vee C$  sowie  $\{\neg B, \neg C\} \vdash \neg(B \vee C)$ .
    - $\varphi(B \rightarrow C) = B \rightarrow C$  gdw.  $\hat{\varphi}(B) = 0$  oder  $\hat{\varphi}(C) = 1$ .  
Z.z.  $\neg B \vdash B \rightarrow C$  und  $C \vdash B \rightarrow C$  sowie  $\{B, \neg C\} \vdash \neg(B \rightarrow C)$ .
- $\star \in \{\vee, \wedge\}$ : trivial bzw. De Morgan; Rest umseitig.

## Beweis (Fortsetzung)

- |    |                         |                 |
|----|-------------------------|-----------------|
| 0. | $B$                     | Prämisse        |
| 1. | $\left[ \neg B \right.$ | Ann.            |
| 2. | $\quad \perp$           | $(\neg e), 0,1$ |
| 3. | $\neg\neg B$            | $(\neg i), 1-2$ |

- |    |                    |                        |
|----|--------------------|------------------------|
| 0. | $C$                | Prämisse               |
| 1. | $\left[ B \right.$ | Ann.                   |
| 2. | $\quad B \wedge C$ | $(\wedge i), 1,0$      |
| 3. | $\quad C$          | $(\wedge e), 3$        |
| 4. | $B \rightarrow C$  | $(\rightarrow i), 1-3$ |

- |    |                                  |                        |
|----|----------------------------------|------------------------|
| 0. | $B$                              | Prämisse               |
| 1. | $\neg C$                         | Prämisse               |
| 2. | $\left[ B \rightarrow C \right.$ | Ann.                   |
| 3. | $\quad C$                        | $(\rightarrow e), 0,2$ |
| 4. | $\quad \perp$                    | $(\neg e), 3,1$        |
| 5. | $B \rightarrow C$                | $(\rightarrow i), 2-4$ |

- |    |                    |                        |
|----|--------------------|------------------------|
| 0. | $\neg B$           | Prämisse               |
| 1. | $\left[ B \right.$ | Ann.                   |
| 2. | $\quad \perp$      | $(\neg e), 1,0$        |
| 3. | $\quad C$          | $(\perp e), 2$         |
| 4. | $B \rightarrow C$  | $(\rightarrow i), 1-3$ |



## Lemma

Mit  $\Gamma \cup \{B\} \vdash A$  und  $\Gamma \cup \{\neg B\} \vdash A$  gilt auch  $\Gamma \vdash A$ .

## Beweis.

- |    |                 |                         |
|----|-----------------|-------------------------|
| 0. | $B \vee \neg B$ | LEM                     |
| 1. | [ $B$           | Ann.                    |
| 2. | [ $A$           | $(\rightarrow e)$ , 3,0 |
| 3. | [ $\neg B$      | Ann.                    |
| 4. | [ $A$           | $(\rightarrow e)$ , 5,1 |
| 5. | $A$             | $(\vee e)$ , 2,3-4,5-6  |



Der [Beweis](#) der 0-Vollständigkeit von  $\mathcal{K}_0$  funktioniert nun auch für  $\mathcal{K}_{\text{nat}}$ .  
 Mit Hilfe des Kompaktheitssatzes folgt sofort die Vollständigkeit:

## Satz

Aus  $\Gamma \models A$  folgt  $\Gamma \vdash A$ .



# Die Korrektheit von $\mathcal{K}_{\text{nat}}$ revisited

- ▷ In expliziten nicht hybriden  $\mathcal{K}_0$ -Beweisen ist aufgrund der Axiome des Hilbert-Kalküls jede Zeile eine Tautologie.
- ▷ Aufgrund der eingebauten Möglichkeit zur Schachtelung ist die Situation in  $\mathcal{K}_{\text{nat}}$  komplizierter. Dafür braucht der Fall  $\Gamma = \emptyset$  nicht gesondert behandelt zu werden.
- ▷ Wir wollen eine  $\mathcal{K}_{\text{nat}}$ -Ableitung für  $\Gamma \vdash G$ , mit  $\Gamma$  endlich, so umschreiben, dass Zeile  $i$  die Form  $\Gamma_i \vdash A_i$  erhält, wobei  $\Gamma_i$  die Menge der **in Position  $i$  aktuellen Prämissen und Annahmen** ist.
  - Auf dem äußeren Level gilt immer  $\Gamma_i = \Gamma$ .
  - Mit Beginn/Ende jeder linken Klammer nimmt die Anzahl der aktuellen Annahmen um eins zu bzw. ab. Insbesondere bestimmt  $|\Gamma_i - \Gamma|$  die Schachtelungstiefe der Zeile  $i$ . Die eckigen Klammern können entfallen.

Als Beispiel betrachten wir den obigen Beweis für (Ax3):

## Beispiel

0.	$\{\neg B \rightarrow \neg A\} \Vdash \neg B \rightarrow \neg A$	Ann.
1.	$\{A, \neg B \rightarrow \neg A\} \Vdash A$	Ann.
2.	$\{\neg B, A, \neg B \rightarrow \neg A\} \Vdash \neg B$	Ann.
3.	$\{\neg B, A, \neg B \rightarrow \neg A\} \Vdash \neg A$	$(\rightarrow e)$ , 2,0
4.	$\{\neg B, A, \neg B \rightarrow \neg A\} \Vdash \perp$	$(\neg e)$ , 1,3
5.	$\{A, \neg B \rightarrow \neg A\} \Vdash \neg\neg B$	$(\neg i)$ , 2-4
6.	$\{A, \neg B \rightarrow \neg A\} \Vdash B$	$(DNE)$ , 5
7.	$\{\neg B \rightarrow \neg A\} \Vdash A \rightarrow B$	$(\rightarrow i)$ , 1-6
8.	$\Vdash (\neg B \rightarrow \neg A) \rightarrow A \rightarrow B$	$(\rightarrow i)$ , 0-7

Jede Zeile enthält eine korrekte Aussage über die Ableitbarkeit  $\Vdash$  in  $\mathcal{K}_{\text{nat}}$ . In mit "Ann." markierten Zeilen gehört die rechte Formel zur linken Menge. Sonst liegt eine logische Regel oder eine frühere Ableitung zugrunde.



## Satz

$\Gamma \vdash G$  impliziert  $\Gamma \models G$ .

## Beweis

Mit Hilfe der Ergebnisse aus dem Semantik-Kapitel lässt sich leicht zeigen:

- ▷  $\Gamma \models G$  und  $\Gamma \models H$  impliziert  $\Gamma \models G \wedge H$ .
- ▷  $\Gamma \models G \wedge H$  impliziert  $\Gamma \models G$  und  $\Gamma \models H$ .
- ▷  $\Gamma \cup \{G\} \models H$  impliziert  $\Gamma \models G \rightarrow H$ .
- ▷  $\Gamma \models G$  und  $\Gamma \models G \rightarrow H$  impliziert  $\Gamma \models H$ .
- ▷  $\Gamma \models G$  oder  $\Gamma \models H$  impliziert  $\Gamma \models G \vee H$ .
- ▷  $\Gamma \models G \vee H$  und  $\Gamma \cup \{G\} \models K$  sowie  $\Gamma \cup \{H\} \models K$  impliziert  $\Gamma \models K$ .
- ▷  $\Gamma \cup \{G\} \models \perp$  impliziert  $\Gamma \models \neg G$ .
- ▷  $\Gamma \models G$  und  $\Gamma \models \neg G$  impliziert  $\Gamma \models \perp$ .

## Beweis, Fortsetzung

- ▷  $\Gamma \models \perp$  impliziert  $\Gamma \models G$ .
- ▷  $\Gamma \models \neg\neg G$  impliziert  $\Gamma \models G$

Dies sind die semantischen Versionen der Regeln für  $\mathcal{K}_{\text{nat}}$ .

Für  $\Gamma \vdash G$  betrachte die wie oben umgeschriebene Ableitung.

**Induktion** über die Anzahl  $k$  der Schritte (=Regel-Anwendungen, keine Abkürzungen aufgrund früherer Ergebnisse) in  $\mathcal{K}_{\text{nat}}$ -Ableitungen zeigt nun, dass wir in jeder Zeile die Relation  $\vdash$  durch  $\models$  ersetzen können.  $\square$

Dies legt nahe ein Kalkül zu entwickeln, das Ausdrücke der Form  $\Gamma \vdash G$  direkt manipuliert.

# Gentzens Sequenzen-Kalkül, Vorbereitung

Gentzens ▶ zweites System war ursprünglich als technisches Hilfsmittel zum Beweis der Konsistenz der Prädikatenlogik gedacht, hat sich aber in vielen Bereichen der Logik als äußerst nützlich erwiesen.

Abstraktion des oben beschriebenen Prozesses mutiert das Relationssymbol  $\vdash$  zu einem **Trennsymbol der Syntax**; wir verwenden nun wieder  $\vdash$ .

Syntaktische Bausteine sind zunächst(!) Ausdrücke der Form  $\Gamma \vdash H$  mit  $\Gamma \in (\mathcal{F}_{\text{nat}})^*$ , sog. **einseitige Sequenzen** (engl. **sequents**, auch **judgements** genannt). Den Zusammenhang mit den oben verwendeten endlichen Mengen auf der linken Seite vermitteln sog. **strukturellen Regeln**, informell

- ▷ Vertauschung (engl. “Exchange”): Prämissen-Reihenfolge irrelevant;
- ▷ Kontraktion (engl. “Contraction”): Prämissen-Wiederholung irrelevant;
- ▷ Verdünnung (engl. “Weakening” oder “Thinning”): Vergrößerung um überflüssige Prämissen zulässig.

# Strukturelle Regeln des ND-Sequenzen-Kalküls

Mittels der bekannten Bruch-Notation erhält man nun:

$$\frac{\Gamma, G, F \vdash H}{\Gamma, F, G \vdash H} \text{ (xch)} \quad , \quad \frac{\Gamma, F, F \vdash H}{\Gamma, F \vdash H} \text{ (ctr)} \quad , \quad \frac{\Gamma \vdash H}{\Gamma, F \vdash H} \text{ (wkg)}$$

- ▷ (xch) erlaubt es zunächst, die aktuellen Prämissen als endliche Multi-Mengen aufzufassen, statt als Tupel;
- ▷ (ctr) erlaubt es dann, diese Multi-Mengen zu endlichen Mengen „einzudampfen“;
- ▷ (wkg) erlaubt es schließlich, Prämissenmengen bei Bedarf zu vergrößern (und damit zu verdünnen). Wie oben gesehen, lassen sich Prämissenmengen von Zeilen verschiedener Schachtelungstiefe so vereinheitlichen.

Übertragung der  $\mathcal{K}_{\text{nat}}^-$ -Regeln eliminiert die Sonderstellung der Regeln mit Fernwirkung. Dafür kommt ein Axiom-Schema hinzu:

## Logische Regeln des ND-Sequenzen-Kalküls

$$\frac{}{\Gamma, F, \Delta \vdash F} \text{ (ax)}$$

	Introduktion	Elimination
$\wedge$	$\frac{\Gamma \vdash G \quad \Gamma \vdash H}{\Gamma \vdash G \wedge H} (\wedge i)$	$\frac{\Gamma \vdash G \wedge H}{\Gamma \vdash G} (\wedge e), \frac{\Gamma \vdash G \wedge H}{\Gamma \vdash H} (\wedge e)$
$\rightarrow$	$\frac{\Gamma, G \vdash H}{\Gamma \vdash G \rightarrow H} (\rightarrow i)$	$\frac{\Gamma \vdash G \quad \Gamma \vdash G \rightarrow H}{\Gamma \vdash H} (\rightarrow e)$
$\vee$	$\frac{\Gamma \vdash G}{\Gamma \vdash G \vee H} (\vee i), \frac{\Gamma \vdash H}{\Gamma \vdash G \vee H} (\vee i)$	$\frac{\Gamma \vdash G \vee H \quad \Gamma, G \vdash K \quad \Gamma, H \vdash K}{\Gamma \vdash K} (\vee e)$
$\neg$	$\frac{\Gamma, F \vdash \perp}{\Gamma \vdash \neg F} (\neg i)$	$\frac{\Gamma \vdash F \quad \Gamma \vdash \neg F}{\Gamma \vdash \perp} (\neg e)$
$\perp$		$\frac{\Gamma \vdash \perp}{\Gamma \vdash G} (\perp e)$

Ein Analogon zur Regel (DNE), die bei der Suche nach Normalformen beliebiger  $\mathcal{K}_{\text{nat}}$ -Beweise gestört hatte, bzw. zu (LEM) oder (CTR), fehlt, also ist der bisher skizzierte Kalkül intuitionistisch.

Gentzens geniale Idee zur Behandlung klassischer Logik mittels Sequenzen im Kalkül  $\mathcal{K}_{\text{seq}}$  war die Verwendung **zweiseitiger Sequenzen** der Form  $\Gamma \vdash \Delta$ , mit endlichen Formelmengen  $\Gamma, \Delta$ . Eine solche Sequenz soll ableitbar sein, wenn  $\bigwedge \Gamma \rightarrow \bigvee \Delta$  allgemeingültig ist.

Die strukturellen Regeln werden zu links- und rechtsseitigen Varianten verdoppelt. In den obigen logischen Regeln treten alle Junktoren rechts von  $\vdash$  auf. Bei zweiseitigen Sequenzen würde man aber auch Regeln mit Junktoren links von  $\vdash$  erwarten.

Die bisherigen Einführungs-Regeln lassen sich leicht in zweiseitige Versionen überführen, nun **Rechts-Introduktionen** genannt (beachte auch  $\perp = \bigvee \emptyset$ ). Beim Ersetzen der bisherigen Eliminierungen durch **Links-Introduktionen** beachte man die Dualität zwischen  $\wedge$  und  $\vee$  und nutze die klassische Ersetzung von  $\rightarrow$  durch  $\neg$  und  $\vee$  als Motivation:

Strukturelle Regeln für  $\mathcal{K}_{\text{seq}}$ 

▷ Exchange:

$$\frac{\Gamma \vdash \Delta_0, A, B, \Delta_1}{\Gamma \vdash \Delta_0, B, A, \Delta_1} \quad (X-R) \qquad \frac{\Gamma_0, A, B, \Gamma_1 \vdash \Delta}{\Gamma_0, B, A, \Gamma_1 \vdash \Delta} \quad (X-L)$$

▷ Contraction:

$$\frac{\Gamma \vdash \Delta_0, A, A, \Delta_1}{\Gamma \vdash \Delta_0, A, \Delta_1} \quad (C-R) \qquad \frac{\Gamma_0, A, A, \Gamma_1 \vdash \Delta}{\Gamma_0, A, \Gamma_1 \vdash \Delta} \quad (C-L)$$

▷ Weakening:

$$\frac{\Gamma \vdash \Delta_0, \Delta_1}{\Gamma \vdash \Delta_0, A, \Delta_1} \quad (W-R) \qquad \frac{\Gamma_0, \Gamma_1 \vdash \Delta}{\Gamma_0, A, \Gamma_1 \vdash \Delta} \quad (W-L)$$

# Erste logische Regeln für $\mathcal{K}_{\text{seq}}$

$$\overline{\Gamma, F \vdash \Delta, F} \quad (\text{AX})$$

	R	L
$\wedge$	$\frac{\Gamma \vdash \Delta, G \quad \Gamma \vdash \Delta, H}{\Gamma \vdash \Delta, G \wedge H} \quad (\wedge R)$	$\frac{\Gamma, G, H \vdash \Delta}{\Gamma, G \wedge H \vdash \Delta} \quad (\wedge L)$
$\rightarrow$	$\frac{\Gamma, G \vdash \Delta, H}{\Gamma \vdash \Delta, G \rightarrow H} \quad (\rightarrow R)$	$\frac{\Gamma \vdash \Delta, G \quad \Gamma, H \vdash \Delta}{\Gamma, G \rightarrow H \vdash \Delta} \quad (\rightarrow L)$
$\vee$	$\frac{\Gamma \vdash \Delta, G, H}{\Gamma \vdash \Delta, G \vee H} \quad (\vee R)$	$\frac{\Gamma, G \vdash \Delta \quad \Gamma, H \vdash \Delta}{\Gamma, G \vee H \vdash \Delta} \quad (\vee L)$
$\neg$	$\frac{\Gamma, G \vdash \Delta}{\Gamma \vdash \Delta, \neg G} \quad (\neg R)$	$\frac{\Gamma \vdash \Delta, G}{\Gamma, \neg G \vdash \Delta} \quad (\neg L)$



# Anmerkungen

Trotz ihrer kompliziert wirkenden Gestalt weisen die obigen Regeln eine Reihe von Zusammenhängen auf:

- ▷ In Anbetracht der Tatsache, dass der linke Teil einer Sequenz implizit eine Konjunktion darstellt, und der rechte Teil eine Disjunktion, sind die Regeln  $(\wedge R)$  und  $(\vee L)$  zueinander dual, ebenso  $(\vee R)$  und  $(\wedge L)$ .
- ▷ Da  $\perp$  neutral bzgl. Disjunktion ist und aufgrund von  $\neg F \equiv F \rightarrow \perp$  lässt sich  $(\neg R)$  aus  $(\rightarrow R)$  herleiten:

$$\frac{\Gamma, G \vdash \Delta, \perp}{\Gamma \vdash \Delta, G \rightarrow \perp} (\rightarrow R) \quad \text{liefert} \quad \frac{\Gamma, G \vdash \Delta}{\Gamma \vdash \Delta, \neg G} (\neg R)$$

- ▷ Da  $\perp$  absorbierend bzgl. Konjunktion ist, gilt  $\Gamma, \perp \vdash \Delta$  trivialerweise immer; damit lässt sich  $(\neg L)$  aus  $(\rightarrow L)$  herleiten:

$$\frac{\Gamma \vdash \Delta, G \quad \Gamma, \perp \vdash \Delta}{\Gamma, G \rightarrow \perp \vdash \Delta} (\rightarrow L) \quad \text{liefert} \quad \frac{\Gamma \vdash \Delta, G}{\Gamma, \neg G \vdash \Delta} (\neg L)$$

Warum  $\mathcal{K}_{\text{seq}}$  die klassische Logik beschreibt

## Beispiel (LEM)

- |    |                        |               |
|----|------------------------|---------------|
| 0. | $A \vdash A$           | Axiom         |
| 1. | $\vdash A, \neg A$     | $(\neg R), 0$ |
| 2. | $\vdash A \vee \neg A$ | $(\vee R), 1$ |

## Beispiel (DNE)

- |    |                                   |                      |
|----|-----------------------------------|----------------------|
| 0. | $A \vdash A$                      | Axiom                |
| 1. | $\vdash A, \neg A$                | $(\neg R), 0$        |
| 2. | $\neg\neg A \vdash A$             | $(\neg L), 1$        |
| 3. | $\vdash \neg\neg A \rightarrow A$ | $(\rightarrow R), 2$ |

# Was fehlt noch in $\mathcal{K}_{\text{seq}}$ ?

Analog zu den Regeln aus  $\mathcal{R}_{\text{nat}}^-$  lassen sich eine oder mehrere Sequenzen zu einer neuen transformieren, wobei die Blockstruktur entfällt.

Es fällt auf, dass die logischen Regeln sämtlich zu komplexeren logischen Formeln im „Nenner“ führen. Damit lassen sich nicht alle Ableitungen von  $\mathcal{K}_{\text{nat}}$  nachspielen, etwa die (ziemlich sinnlose) Ableitung:

$  \begin{array}{ll}  \mathcal{K}_{\text{nat}} & \vdots \\  n. & G \\  n+1. & H \\  n+2. & G \wedge H \quad (\wedge i), n, n+1 \\  n+3. & G \quad (\wedge e), n+2  \end{array}  $		$  \begin{array}{ll}  \mathcal{K}_{\text{seq}} & \vdots \\  n. & \Gamma \vdash G \\  n+1. & \Gamma \vdash H \\  n+2. & \Gamma \vdash G \wedge H \quad (\wedge R), n, n+1 \\  & ??? \\  m. & G \vdash G \quad \text{Axiom} \\  m+1. & G \wedge H \vdash G \quad (\wedge L), m  \end{array}  $
---	--	--

Wie will man in  $\mathcal{K}_{\text{seq}}$  die Sequenzen  $n+2$  und  $m+1$  verbinden?

# Die Schnittregel

Gentzen behalf sich, indem er  $\mathcal{K}_{\text{seq}}$  durch Einführung einer neuen strukturellen Regel, der **Schnittregel**, zu  $\mathcal{K}_{\text{seq}}^+$  erweiterte:

$$\frac{\Gamma_0 \vdash \Delta_0, A \quad A, \Gamma_1 \vdash \Delta_1}{\Gamma_0, \Gamma_1 \vdash \Delta_0, \Delta_1} \quad (\text{CUT})$$

Mit ihrer Hilfe lässt sich oben aus den Sequenzen  $\Gamma \vdash G \wedge H$  und  $G \wedge H \vdash G$  wie gewünscht  $\Gamma \vdash G$  erhalten.

Einzig durch die Schnittregel können (Teil-)Formeln aus einem Beweis verschwinden. Um die einzige widersprüchliche Sequenz  $\vdash$  bzw.  $\emptyset \vdash \emptyset$  abzuleiten, müßte die Schnittregel zwingend angewendet werden.

Als Gegenstück zur Existenz von  $\mathcal{K}_{\text{nat}}^-$ -Beweisen in Normalform mit der Teilformel-Eigenschaft für den intuitionistischen Teil der Aussagenlogik konnte Gentzen für den zweiseitigen Sequenzen-Kalkül zeigen:

# Cut-Elimination

## Satz (Gentzens Hauptsatz, ohne Beweis)

*Zu jedem  $\mathcal{K}_{\text{seq}}^+$ -Beweis  $\Gamma \vdash \Delta$  existiert ein (CUT)-freier  $\mathcal{K}_{\text{seq}}$ -Beweis von  $\Delta$  aus  $\Gamma$ , und dieser kann algorithmisch aus dem ursprünglichen Beweis konstruiert werden.* □

**Beweisidee:** Anwendungen der Schnittregel in einem Baum-förmigen Beweis, oberhalb derer keine weitere Schnittregel auftritt, in Richtung der Blätter (=Axiome) zu „verschieben“, wo sie sich schließlich „auflösen“.

## Korollar

Der Sequenzenkalkül ist konsistent, d.h., die beidseitig leere Sequenz  $\vdash$  ist nicht aus Axiomen ableitbar. □

# Kapitel 7

## Algorithmen für die Aussagenlogik

# Übersicht

Zum Nachweis von  $\Gamma \models A$  kann man anstelle von  $\Gamma \vdash A$  natürlich auch die Nichterfüllbarkeit von  $\Gamma \cup \{\neg A\}$  überprüfen. Aufgrund des KPS lässt sich dies selbst bei unendlichem  $\Gamma$  (z.B. bei einer [Herbrand Expansion](#)) in endlich vielen Schritten feststellen, im Gegensatz zur Erfüllbarkeit. Daher ist das Problem der Unerfüllbarkeit **semi-entscheidbar**.

Wir stellen drei Syntax-basierte Algorithmen vor, mit deren Hilfe die Nichterfüllbarkeit von Formel(menge)n häufig schneller gezeigt werden kann, als mittels Wahrheitstabellen (brute force) oder deduktiver Ableitungen. Im ungünstigsten Fall ist ihre Laufzeit aber immer noch exponentiell. Bei erfüllbaren endlichen Mengen werden erfüllende Belegungen gefunden.

Beliebige Formelmengen über  $\mathcal{J}_1 = \{\neg, \wedge, \vee, \rightarrow\}$  lassen sich mit **semantischen Tableaus** behandeln, der **Davis-Putnam Algorithmus** erfordert Formeln in **Negations-Normalform (NNF)**, und die **Resolutionsmethode** in **konjunktiver Normalform (KNF)**. Wir behandeln diese Normalformen, ihre Konstruktion und das Phänomen der **Erfüllbarkeitsäquivalenz**.

# Klassifikation und Zerlegung von Formeln über $\mathcal{J}_1$

- ▷ **Literale**, d.h., Atome in  $\mathcal{A}$  oder deren Negationen;
- ▷ **führende doppelte Negationen** – überflüssig, werden sofort eliminiert;
- ▷ bis auf Äquivalenz binäre Konjunktionen, genannt  **$\alpha$ -Formeln**:

$$\frac{A \wedge B}{A, B} \quad , \quad \frac{\neg(A \vee B) \quad \neg(A \rightarrow B)}{\neg A, \neg B}$$

Sind beide  **$\alpha$ -Teilchen** im „Nenner“ wahr, so auch der „Zähler“.

- ▷ bis auf Äquivalenz binäre Disjunktionen, genannt  **$\beta$ -Formeln**:

$$\frac{A \vee B}{A | B} \quad , \quad \frac{\neg(A \wedge B)}{\neg A | \neg B} \quad , \quad \frac{A \rightarrow B}{\neg A | B}$$

Ist ein  **$\beta$ -Teilchen** im „Nenner“ wahr, so auch der „Zähler“.



# Tableau-Methode (TM): Übersicht

- ▷ Die iterative Zerlegung einer Formel in ihre **Teilchen** terminiert nach endlich vielen Schritten mit Literalen.
- ▷ Um deren Erfüllbarkeit mit der der Ursprungsformel in Beziehung setzen zu können, **genügt die Menge der iterierten Teilchen nicht**.
- ▷ Da die Wahrheit **eines**  $\beta$ -Teilchens die seiner  $\beta$ -Formel garantiert, bietet es sich an, die entstehenden Teilchen in einen dynamisch wachsenden **binären Baum** mit **Formelmengen** als Knoten zu sortieren. **Das funktioniert auch, wenn man mit einer Formelmenge  $\Gamma$  beginnt**.
- ▷ Die interessanten Teilchen-Teilmengen neben den Knoten sind dann die Vereinigungen der Knoten-Mengen entlang von Ästen des Baums.
- ▷ Finden sich in den Knoten-Mengen entlang eines Astes Formeln  $B$  und  $\neg B$ , gilt der Ast als **geschlossen**. Der Zweig des späteren Knotens liefert keine weiteren Erkenntnisse und kann „eingefroren“ werden.
- ▷  $\Gamma$  ist unerfüllbar gdw. wenn alle Äste geschlossen werden können.

## Definition

- 1  $\mathcal{F}^{\neg\neg}[\mathcal{A}] \subseteq \mathcal{F}[\mathcal{A}]$  besteht aus genau den Formeln, die **nicht** mit einer doppelten Negation **beginnen**.
- 2  $\Gamma \subseteq \mathcal{F}^{\neg\neg}[\mathcal{A}]$  heißt **gesättigt**, wenn mit jeder  $\alpha$ -Formel aus  $\Gamma$  auch beide  $\alpha$ -Teilchen modulo  $\neg\neg$  zu  $\Gamma$  gehören. Die kleinste gesättigte Obermenge  $\Gamma^{<\alpha>}$  von  $\Gamma$  heißt  **$\alpha$ -Hülle**.
- 3  $\Gamma \subseteq \mathcal{F}^{\neg\neg}[\mathcal{A}]$  heißt **vollständig**, wenn  $\Gamma$  gesättigt ist und mit jeder  $\beta$ -Formel auch mindestens ein  $\beta$ -Teilchen enthält

- ▷  $\Gamma$  als Wurzel wird injektiv durchnummeriert,  $G_i$ ,  $i < n$  oder  $i \in \mathbb{N}$ ;
- ▷  $G_i$  wird vor  $G_{i+1}$  vollständig zerlegt und die Teilchen werden platziert;
- ▷ bis auf evtl. die Wurzel bleiben dabei alle Knotenmengen endlich;
- ▷ sobald eine Knotenmenge gesättigt ist, bleibt sie stabil;
- ▷ Widersprüche entlang von Ästen werden registriert: Abschluß!
- ▷ die Literale in offenen vollständigen Ästen liefern einen Erfüller von  $\Gamma$ .

# Vorüberlegung zur praktischen Tableau-Konstruktion

## Vereinbarung zur Vereinfachung

- ▷ Stimmen für  $G \in \Gamma$  beide  $\alpha$ - bzw.  $\beta$ -Teilchen überein, so ersetzen wir  $G$  direkt durch das einfachere Teilchen.
- ▷ Widersprüche werden nur unter den auftretenden Literalen gesucht.

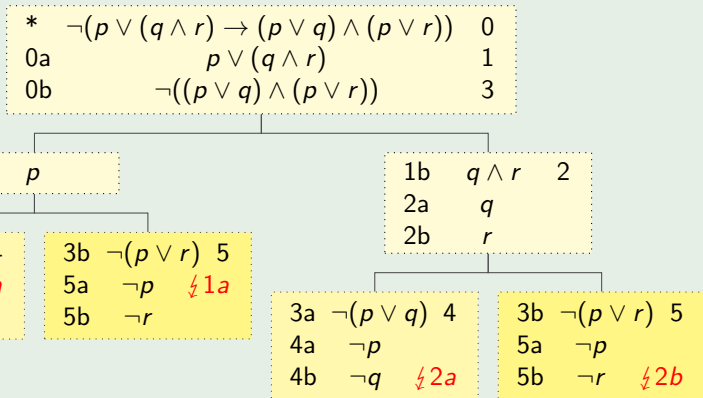
Ein Algorithmus zur Konstruktion eines Tableaus für potentiell unendliches  $\Gamma$  kann zu jedem Zeitpunkt immer nur endlich viele Formeln im Blick haben.

Die Reihenfolge der Abarbeitung wird man nur schwer vorschreiben können, dafür lassen sich bei Bedarf später Strategien formulieren.

Zwecks **Buchführung** werden wir jede Formel bis zu zweifach markieren:

- rechts, sofern es sich nicht um ein Literal handelt, mit der fortlaufenden Nummer  $k$  des Arbeitsschritts, in dem sie zerlegt wird;
- links mit einem Verweis, dass sie erfasst ist, bzw. auf den Arbeitsschritt ihrer Entstehung.

Beispiel ( $\Gamma = \{\neg(p \vee (q \wedge r) \rightarrow (p \vee q) \wedge (p \vee r))\}$  ist nicht erfüllbar.)

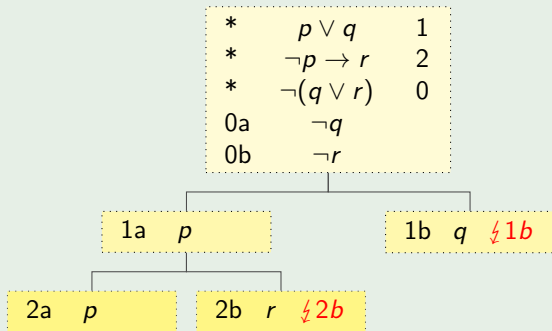


Wir belassen die  $\alpha$ -Teilchen im aktuellen Knoten. (Andere Varianten der Tableau-Methode verschieben sie in die nachfolgenden aktuellen Blätter.)

# Praktische Konstruktion des Tableaus für $\Gamma \subseteq \mathcal{F}[A]$

- 1  $\Gamma$  bildet zunächst die potentiell unendliche Wurzelmenge.
- 2 Wahl einer unbearbeiteten Formel  $A$ , ggf. mit  $*$  als erfasst markieren.
- 3 Ist  $A$  kein Literal und wird in Schritt  $k$  regel-konform zerlegt, werden die Teilchen links mit  $ka$  bzw.  $kb$  als erfasst markiert:
  - beide  $\alpha$ -Teilchen landen hier direkt im Knoten von  $A$  (bei anderer Strategie in allen aktuellen Blättern unter dem Knoten von  $A$ );
  - die (nach Vereinbarung verschiedenen)  $\beta$ -Teilchen starten unter jedem aktuellen auf den Knoten von  $A$  folgenden Blatt je ein neues Blatt.
- 4 Treten entlang eines Astes erfasste(!) Literale  $p$  und  $\neg p$  auf wird dieser als **geschlossen** markiert und der Zweig des tiefer liegenden betroffenen Knotens von der weiteren Bearbeitung ausgeschlossen.
- 5 Zum raschen Auffinden evtl. widersprüchlicher Literale zerlegt man jede  $\Gamma$ -Formel vollständig, bevor die nächste an die Reihe kommt.
- 6 Jedes Element von  $\Gamma$  wird nach endlich vielen Schritten bearbeitet.

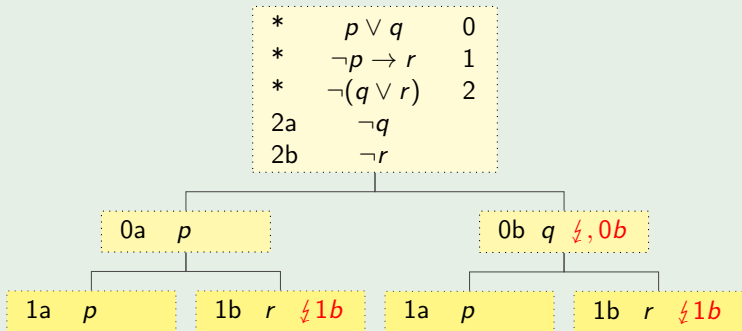
Beispiel ( $\Gamma = \{A_0 = p \vee q, A_1 = \neg p \rightarrow r, A_2 = \neg(q \vee r)\}$  ist erfüllbar.)



In Position (2a) wurde eine doppelte Negation sofort eliminiert.

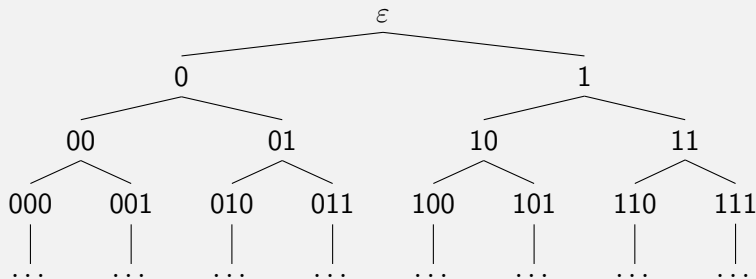
Entlang des linken Astes macht die Belegung  $p \mapsto 1, q \mapsto 0, r \mapsto 0$  die Literale in Position (2a und 1a), (0a) bzw. (0b), und damit  $\Gamma$  wahr.

## Beispiel (wie oben, andere Reihenfolge der Bearbeitung)



# Einschub: $\mathbb{B}^*$ als Baum betrachtet

Wir fassen die Menge  $\mathbb{B}^* = \bigcup\{\mathbb{B}^n : n \in \mathbb{N}\}$  als unendlichen binären Baum mit Wurzel  $\varepsilon$  auf:



Eine Teilmenge  $W \subseteq \mathbb{B}^*$  ist **Präfix-abgeschlossen**, wenn die Präfixe aller Elemente  $w \in W$  ebenfalls zu  $W$  gehören, d.h., alle Knoten entlang des Pfades von  $\varepsilon$  nach  $w$ , und **gerade**, wenn für alle  $w \in \mathbb{B}^*$  gilt  $w0 \in \mathcal{B}(\tau)$  gdw.  $w1 \in \mathcal{B}(\tau)$ .



# Warum funktioniert das obige Verfahren für $\Gamma \subseteq \mathcal{F}^{\neg\neg}[\mathcal{A}]$ ?

## Definition

Ein **Tableau** für  $\Gamma$  ist eine Abbildung  $\mathbb{B}^* \xrightarrow{\tau} \mathbf{P}(\mathcal{F}^{\neg\neg}[\mathcal{A}])$ , so dass

- ▷ das Urbild  $\mathcal{B}(\tau)$  der nichtleeren Formelmengen Präfix-abgeschlossen und gerade ist;
- ▷  $\Gamma \subseteq \tau(\varepsilon) \subseteq \Gamma^{<\alpha>}$  die einzige potentiell unendliche Knotenmenge ist;
- ▷ für jedes  $\varepsilon \neq w \in \mathcal{B}(\tau)$  ein  $\beta$ -Teilchen  $B \in \tau(w)$  einer  $\beta$ -Formel aus einem echten Vorgängerknoten existiert mit  $\tau(w) \subseteq \{B\}^{<\alpha>}$ .

Ein **Ast**  $\Theta$  von  $\mathcal{B}(\tau)$  (**maximale lineare Präfix-geordnete Teilmenge**) heißt

- ▷ **abgeschlossen**, falls  $\bigcup \tau[\Theta]$  eine Formel und ihre Negation enthält; andernfalls heißt  $\Theta$  **offen**;

Ein Tableau heißt **abgeschlossen** falls jeder Ast abgeschlossen ist, und **vollständig**, wenn **die Vereinigung über jeden offenen Ast** vollständig ist.

# Die Existenz vollständiger Tableaus

## Lemma

Jedes Tableau  $\tau$  für  $\Gamma$  kann vervollständigt werden.

## Beweis.

Klar für  $|\Gamma|$  endlich. Sonst zähle die bisher unbearbeiteten Nicht-Literale in  $\tau_{-1} := \tau$  samt ihrer Knoten injektiv auf:  $\langle A_i, w_i \rangle$ ,  $i \in \mathbb{N}$ . Aus  $\tau_{k-1}$  entsteht  $\tau_k$  durch vollständige Zerlegung von  $A_k$  in der Position  $w_k$ . Dann gilt  $\tau_k(w) \subseteq \tau_{k+1}(w)$  für alle  $w \in \mathbb{B}^*$ . Das liefert  $\tau_\infty$  mit

$$\tau_\infty(w) := \bigcup \{ \tau_k(w) : k \in \mathbb{N} \} \quad \text{für } w \in \mathbb{B}^*$$

Jede dieser Mengen in einem offenen Ast ist gesättigt und die Vereinigung über einen offenen Ast ist nach Konstruktion vollständig.  $\square$

Jede Menge  $\Gamma \subseteq \mathcal{F}^{\neg\neg}[\mathcal{A}]$  hat ein **Minimaltableau**  $\tau_*$  mit  $\tau_*(\varepsilon) = \Gamma$  und  $\tau_*(w) = \emptyset$  falls  $w \neq \varepsilon$ , von dem aus man starten kann.

## Lemma (Hintikka)

Für vollständige Tableau-Astmengen gilt: „erfüllbar“ = „offen“.

### Beweis.

„ $\Rightarrow$ “ ist klar. Umgekehrt sei  $\Theta$  offen.  $\varphi$  möge genau die Atome  $p$  mit  $\neg p \in \bigcup \tau[\Theta]$  auf 0 abbilden. Induktion über den Aufbau der Formeln in  $\bigcup \tau[\Theta]$  (vollständig!) und die Abhängigkeit derer Wahrheitswerte von denen ihrer Teilchen zeigt  $\varphi \in (\bigcup \tau[\Theta])^\triangleright$ . □

Die ursprüngliche Tableau-Methode (um 1955) markiert Knoten sub-binärer Bäume mit einzelnen Formeln statt Formelmengen. Sie geht auf Beth<sup>7</sup> und (unabhängig) Hintikka<sup>8</sup> zurück. Smullyans<sup>9</sup> Vereinfachung (1968, 1995) machte sie populär. Die maximale linearen Ketten bis zu den Verzweigungsknoten entsprechen im Wesentlichen den hier verwendeten Knotenmengen.

---

<sup>7</sup>Evert Willem Beth (1908–1964)

<sup>8</sup>Jaakko Hintikka (1929–2015)

<sup>9</sup>Raymond Merrill Smullyan (1919–2017)

# Unerfüllbarkeit via Tableaus

## Satz

$\Gamma$  ist unerfüllbar gdw.  $\Gamma$  hat ein abgeschlossenes Tableau.

## Beweis.

Jedes Tableau  $\tau$  für  $\Gamma$  enthält  $\Gamma$  in allen Astmengen. Unerfüllbarkeit überträgt sich auf diese, und nach Hintikkas Lemma sind sie abgeschlossen.

Umgekehrt folgt aus  $\varphi \in \Gamma^\triangleright$  per Induktion über die Wörter in  $\mathbb{B}^*$  die Existenz eines offenen Asts in jedem Tableau  $\tau$  für  $\Gamma$ :

**Anfang:**  $\varphi$  erfüllt  $\Gamma^{<\alpha>} = \tau_\infty(\varepsilon)$  für eine Vervollständigung  $\tau_\infty$  von  $\tau$ .

**Annahme:**  $\tau_\infty(w) \neq \emptyset$  und  $\varphi$  erfüllt  $\bigcup \{ \tau_\infty(u) : u \leq w \}$ .

**Schluss:** Ist  $\tau_\infty(wi)$  leer,  $i < 2$ , bestimmt  $w$  einen offenen Ast für  $\tau_\infty$ .

Sonst existiert ein Präfix  $u \leq w$  und eine  $\beta$ -Formel  $B \in \tau_\infty(u)$  mit  $\tau_\infty(wi) = \{ B_i \}^{<\alpha>}$ ,  $i < 2$ , für ihre  $\beta$ -Teilchen. Wegen  $\varphi(B) = 1$  erfüllt  $\varphi$  nun  $B_k$  für ein  $k < 2$ , und damit ganz  $\tau_\infty(wk) \supseteq \tau(wi)$ .  $\square$

# Rechtfertigung der Tableau-Konstruktion

## Lemma

- 1 Für endliches  $\Gamma \subseteq \mathcal{F}^{\neg\neg}[A]$  terminiert obige Konstruktion.
- 2 Ist  $\Gamma$  unendlich und unerfüllbar, so terminiert die Konstruktion mit einem abgeschlossenen Tableau endlicher Tiefe.

## Beweis.

Der endliche Fall ist klar. Nun sei  $\Gamma$  unendlich und unerfüllbar.

**Annahme:** Die Konstruktion liefert, ausgehend von  $\tau_*$ , eine streng monoton wachsende Folge  $\tau_i$ ,  $i \in \mathbb{N}$ . Deren Vereinigung  $\bar{\tau}$  ist ein unendlicher binärer Baum mit nichtleeren Knotenmengen, hat nach Königs Lemma also einen unendlichen offenen Ast  $\Theta$ . Da jedes Nicht-Literal von  $\bar{\tau}$  bearbeitet wurde, bewirkt die Vervollständigung nichts, folglich ist  $\bar{\tau}$  selber vollständig, speziell also auch der Ast  $\Theta$ . Nach Hintikkas Lemma ist nun  $\bigcup \tau[\Theta] \supseteq \Gamma$  erfüllbar, Widerspruch. □

## Anmerkung

Aufgrund der Assoziativität von Kon- und Disjunktion lassen sich die  $\alpha$ - bzw.  $\beta$ -Regeln von Folie [Folie 150](#) entsprechend verallgemeinern, so dass mehr als zwei Teilchen entstehen. Das liefert natürlich Bäume, die nicht mehr binär sein müssen, was aber nichts Wesentliches ändert.

### Beispiel

- ▷ 3-teilige  $\alpha$ -Formeln:

$$\frac{A \wedge B \wedge C}{A, B, C} \quad , \quad \frac{\neg(A \vee B \vee C)}{\neg A, \neg B, \neg C} \quad , \quad \frac{\neg(A \rightarrow B \rightarrow C)}{A, B, \neg C}$$

- ▷ 3-teilige  $\beta$ -Formeln:

$$\frac{A \vee B \vee C}{A | B | C} \quad , \quad \frac{\neg(A \wedge B \wedge C)}{\neg A | \neg B | \neg C} \quad , \quad \frac{A \rightarrow B \rightarrow C}{\neg A | \neg B | C}$$

# Normalformen

Im Gegensatz zur Tableau-Methode erfordern die nächsten beiden Algorithmen ([Davis-Putnam](#) und [Resolution](#)) Eingaben in einer bestimmten einfachen Gestalt. Dabei beschränken wir uns auf die vollständige Junktormenge  $\mathcal{J}_2 := \{\neg, \wedge, \vee\}$ . Die entsprechenden [Normalformen](#) sind im Hinblick auf den spezifischen Algorithmus zu verstehen; leider gibt es keine universell beste/kleinste/einfachste Darstellung von Formeln über  $\mathcal{J}_2$  (s.u.).

**Achtung:** Bei der Betrachtung der Effizienz von Algorithmen darf die Umwandlung allgemeiner Eingabe(n) in die nötige Normalform nicht vernachlässigt werden. Sie sollte bzgl. Zeit/Platz verglichen mit dem entsprechenden Bedarf des eigentlichen Algorithmus [nicht zu teuer](#) sein.

## Definition

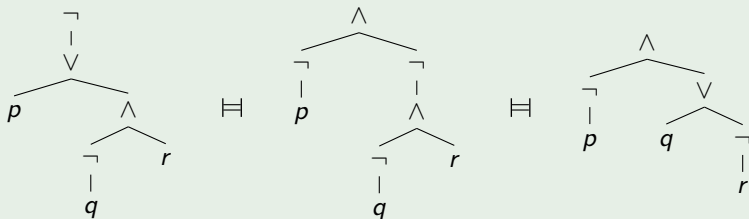
Formeln ohne die Junktoren  $\perp$ ,  $\top$ ,  $\rightarrow$  und  $\leftrightarrow$  und ohne doppelte Negationen liegen in [Boole'scher Normalform \(BNF\)](#) vor. Die entsprechende Teilmenge von  $\mathcal{F}_2[\mathcal{A}]$  bezeichnen wir ebenfalls mit BNF.

## Beispiel

Folgende Formeln lassen sich durch de Morgan'sche Regeln ineinander umformen (die Distributivgesetze vergrößern unnötig die Blätterzahl):

$$\neg(p \vee (\neg q \wedge r)) \quad , \quad (\neg p \wedge \neg(\neg q \wedge r)) \quad , \quad (\neg p \wedge (q \vee \neg r))$$

Die äußeren Formeln sind gleich lang, ihre Syntaxbäume haben 7 Knoten und 6 Kanten, unterscheiden sich aber in der Tiefe:



Die rechte Formel in KNF (s.u.) wird am Nützlichsten sein.



# Umwandlung in BNF

Die Junktoren  $\top$ ,  $\perp$ ,  $\rightarrow$  und  $\leftrightarrow$  bzw. doppelte Negationen lassen sich mittels folgender Äquivalenzen aus Formeln  $A \in \mathcal{F}[\mathcal{A}]$  entfernen:

$$\top \vDash p \vee \neg p \text{ mit } p \notin \mathcal{O}(A)$$

$$\perp \vDash p \wedge \neg p \text{ mit } p \notin \mathcal{O}(A)$$

$$B \rightarrow C \vDash \neg B \vee C$$

$$B \leftrightarrow C \vDash (\neg B \vee C) \wedge (\neg C \vee B)$$

$$\neg\neg B \vDash B$$

## Vereinbarung

Nur die vorletzte Regel kann zu nicht-linearem (sogar exponentiellem) Wachstum in der Länge führen, sofern der Junktor  $\leftrightarrow$  beliebig oft auftreten darf. Nachdem  $\leftrightarrow$  schon hinsichtlich der Monotonie (vergl. [Folie 68](#)) Probleme bereitete, **wollen wir zunächst auf den Junktor  $\leftrightarrow$  verzichten.**

# Negationsnormalform

## Definition (NNF)

**NNF**  $\subseteq$  BNF ist der Abschluß der Menge  $\mathcal{A} + \neg\mathcal{A}$  der **Literale** unter Kon- und Disjunktion.

## Definition

Für  $A \in \mathcal{F}[\mathcal{A}]$  bezeichne  $\|A\|$  die Anzahl der Blätter des Syntaxbaums.

## Lemma (HA!)

Zu jeder Formel  $A \in \mathcal{F}[\mathcal{A}]$  *ohne*  $\leftrightarrow$  existiert eine äquivalente Formel  $B \in \text{NNF}$ , so dass  $\|B\|$  in  $\mathcal{O}(\|A\|)$  liegt, d.h., bis auf eine Konstante linear von  $\|A\|$  abhängt. □

# KNF und DNF für $\mathcal{J}_2 = \{\neg, \wedge, \vee\}$

## Definition

- ▶ Eine Disjunktion von Literalen heißt **Klausel**. Man unterscheidet
  - **positive/negative** Klauseln, in denen alle Literale positiv/negativ sind;
  - **Horn-Klauseln** mit maximal einem positiven Literal;
  - **$k$ -Klauseln**, wenn maximal  $k$  Literale auftreten; im Fall  $k = 1$  spricht man auch von **Unit-Klauseln**.
- ▶ Eine Konjunktion von Klauseln heißt **konjunktive Normalform (KNF)**, speziell  **$k$ -KNF** im Fall von  $k$ -Klauseln. Die entsprechenden Teilmengen von  $\mathcal{F}_2[A]$  bezeichnen wir ebenso, also  $k\text{-KNF} \subseteq \text{KNF} \subseteq \text{NNF}$ .

## Definition

Vertauscht man in der obigen Definition die Rollen von Konjunktion ( $\wedge$ ) und Disjunktion ( $\vee$ ), so erhält man die Begriffe der **co-Klausel** und der **disjunktiven Normalform (DNF)**. Es gilt  $k\text{-DNF} \subseteq \text{DNF} \subseteq \text{NNF}$ .

## Bemerkung (alternative Mengendarstellung für KNF)

Schreibt man Klauseln/KNF-Formeln als Mengen von Literalen/Klauseln,

$$\{\{p, q, r\}, \{p, \neg q\}, \{\neg p, q\}\} \quad \text{statt} \quad (p \vee q \vee r) \wedge (p \vee \neg q) \wedge (\neg p \vee q)$$

lassen sich diese mittels  $\subseteq$  („**Subsumption**“) vergleichen

**Klauseln:**  $K \subseteq L$  impliziert  $K \sqsubseteq L$ , und  $K \cup L = K \vee L$ ;

**KNF-Formeln:**  $F \subseteq G$  impliziert  $G \sqsubseteq F$ , und  $F \cup G = F \wedge G$ .

Kommutativität, Assoziativität und Idempotenz gelten nun automatisch.

## Lemma (KNF-Reduktion)

- ▷ Für Klauseln mit  $K \subseteq L$  gilt  $K \vDash K \wedge L$ .
- ▷ Enthält die Klausel  $K$  komplementäre Literale, so gilt  $K \vDash \top$ . □

Daher kann und sollte man subsumierte und tautologische Klauseln aus einer KNF entfernen, bzw. von weiterer Bearbeitung ausschließen.

## Lemma

Zu jeder Formel  $A \in \text{BNF}$  existiert eine äquivalente Formel  $B \in \text{KNF}$ , so dass  $\|B\|$  in  $\mathcal{O}(2^{\|A\|})$  liegt.

## Beweis.

Der Syntaxbaum von  $\text{NNF}(A)$  hat  $N \in \mathcal{O}(\|A\|)$  Blätter und ist, bis auf eventuelle Negationen von Blättern, streng binär. Daher ist seine Höhe durch  $N - 1$  beschränkt, und die Summe der Entfernungen zweier Blätter von der Wurzel (Astlängen) durch  $N$ . Zieht man mit dem 2.

Distributivgesetz Disjunktionen „nach innen“, kann die Höhe des Baums höchstens auf die Summe zweier Astlängen wachsen, also  $\|B\| \leq 2^N$ .  $\square$

## Lemma (HA!)

Es gibt eine Folge von  $\text{NNF}$ -Formeln  $A_n$ ,  $n \in \mathbb{N}$ , mit  $\|A_n\| = 2n$ , so dass jede logisch äquivalente Formel  $B_n$  in  $\text{KNF}$  mindestens  $2^n = (\sqrt{2})^{\|A_n\|}$  Positionen mit Literalen hat.

# Duale Formeln und einfache Zusammenhänge

## Definition

Die **duale Formel** zu  $A \in \mathcal{F}_2[\mathcal{A}]$  ist gegeben durch

$$\begin{aligned} d(p) &:= p \text{ für } p \in \mathcal{A} & d(\bigwedge_{i < n} B_i) &:= \bigvee_{i < n} d(B_i) \\ d(\neg A) &:= \neg d(A) & d(\bigvee_{i < n} B_i) &:= \bigwedge_{i < n} d(B_i) \end{aligned}$$

## Anmerkung

$\mathcal{F}_2[\mathcal{A}]$  (wie auch BNF) ist eine Algebra für die Signatur  $\{\neg, \wedge, \vee\} \xrightarrow{\text{ar}_2} \mathbb{N}$  mit  $\neg_{/1}$ ,  $\wedge_{/2}$  und  $\vee_{/2}$ . Komposition mit der Bijektion  $\delta$  auf  $\mathcal{J}_2 = \{\neg, \vee, \wedge\}$ , die  $\wedge$  und  $\vee$  vertauscht, liefert eine weitere Signatur, bzgl. der BNF eine Algebra ist. Alternativ können wir neben der kanonischen Interpretation der Junktoren  $\wedge$  und  $\vee$  auf BNF auch eine zweite Interpretation betrachten, bei der die Interpretationen von  $\wedge$  und  $\vee$  vertauscht sind. **In jedem Fall ist  $d$  ein selbstinverser Homomorphismus zwischen diesen verschiedenen Algebren mit derselben Trägermenge!**

## Lemma

- ▷  $A \in \text{KNF}$  impliziert  $\text{NNF}(\neg A) \in \text{DNF}$
- ▷  $A \in \text{KNF}$  genau dann wenn  $d(A) \in \text{DNF}$ . □

## Lemma

- (a)  $(\widehat{\mathbf{1} - \varphi})(d(A)) = 1 - \hat{\varphi}(A)$  für jede Belegung  $\varphi$ .
- (b)  $A$  ist eine Tautologie gdw.  $d(A)$  ist nicht erfüllbar.
- (c)  $A$  ist erfüllbar gdw.  $d(A)$  ist keine Tautologie.
- (d)  $\neg A$  ist erfüllbar gdw.  $d(A)$  ist erfüllbar.
- (e)  $B \sqsubseteq A$  impliziert  $d(A) \sqsubseteq d(B)$ .

## Beweis.

- (a)  $\mathbf{1}$  ist die konstante Belegung mit dem Wert 1, also ist  $\mathbf{1} - \varphi$  die zu  $\varphi$  komplementäre Belegung. Strukturelle Induktion liefert nun:

## Beweis, Fortsetzung.

$$\widehat{(\mathbf{1} - \varphi)}(d(p)) = (\mathbf{1} - \varphi)(p) = 1 - \varphi(p) = 1 - \hat{\varphi}(p)$$

$$\begin{aligned}\widehat{(\mathbf{1} - \varphi)}(d(\neg A)) &= \widehat{(\mathbf{1} - \varphi)}(\neg d(A)) = 1 - \widehat{(\mathbf{1} - \varphi)}(d(A)) \\ &= 1 - (1 - \hat{\varphi}(A)) = 1 - \hat{\varphi}(\neg A)\end{aligned}$$

$$\begin{aligned}\widehat{(\mathbf{1} - \varphi)}(d(B \wedge C)) &= \widehat{(\mathbf{1} - \varphi)}(d(B) \vee d(C)) \\ &= \sup\{1 - \hat{\varphi}(B), 1 - \hat{\varphi}(C)\} \\ &= 1 - \inf\{\hat{\varphi}(B), \hat{\varphi}(C)\} = 1 - \hat{\varphi}(B \wedge C)\end{aligned}$$

Der Fall  $d(B \vee C)$  verläuft dual analog.

- (b) (c) (d) Folgt sofort aus (a) sowie der Beobachtung auf [Folie 165](#).
- (e)  $B \sqsubseteq A$  ist durch  $\hat{\varphi}(B) \leq \hat{\varphi}(A)$  für jedes  $\varphi \in \mathbb{B}^A$  definiert. Mit  $\varphi$  läuft aber auch  $\mathbf{1} - \varphi$  durch alle Belegungen in  $\mathbb{B}^A$ . Wegen  $1 - \hat{\varphi}(A) \leq 1 - \hat{\varphi}(B)$  folgt die Behauptung nun aus (a). □



# Erfüllbarkeit via Elimination von Atomen: Davis-Putnam

## Lemma (HA)

Für  $A \in \mathcal{F}[\mathcal{A}]$  und  $p \in \mathcal{O}(A)$  gilt:  $A$  ist genau dann erfüllbar, wenn  $A[p/\top]$  oder  $A[p/\perp]$  erfüllbar ist. □

Statt einer Wahrheitstabelle für  $A$  mit Belegungen von  $\mathcal{O}(A)$  als Zeilen liefert obiges Lemma binäre „Wahrheitsbäume“ (s.u.) durch sukzessive Substitution der Atome von  $A$  durch  $\top$  bzw.  $\perp$  in geeigneter Reihenfolge.

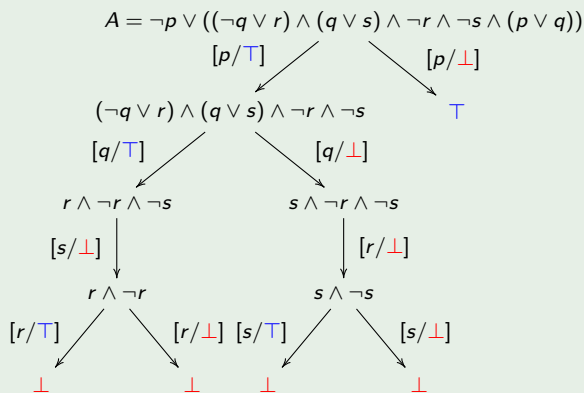
Für  $A \in \text{NNF}$  sind die Substitutionen leicht auswertbar und bleiben in NNF. Und beim Nachweis der Erfüllbarkeit kann man manche Äste ignorieren. Algorithmen, die diese Idee umsetzen und mit Heuristiken weiter verfeinern, sind als **Davis<sup>10</sup>-Putnam<sup>11</sup>-Verfahren** bekannt. Das ursprüngliche Verfahren wurde 1960 veröffentlicht, und noch heute kommen seine Varianten in den schnellsten SAT-Solvern zur Anwendung.

<sup>10</sup>Martin Davis (\*1928)

<sup>11</sup>Hilary Whitehall Putnam (1926-2016)

Nutze, dass  $\top$  und  $\perp$  neutral bzw. absorbierend sind bzgl.  $\wedge$  und  $\vee$ .

### Beispiel (vollständig binärer „Wahrheitsbaum“)



Damit erfüllt jede Belegung mit  $\varphi(p) = 1$  die Formel  $A$ .

## Lemma

Erfüllt  $A \in \text{NNF}$  eine der folgenden Bedingungen

- ▷ (**Unit**)  $A = p \wedge B$  (bzw.  $A = \neg p \wedge B$ ) für ein Atom  $p$ , oder
- ▷ (**Pure Literal**)  $p \in \mathcal{O}(A)$  tritt nur positiv (bzw. negativ) in  $A$  auf, so ist  $A$  genau dann erfüllbar, wenn dies für  $A[p/\top]$  (bzw.  $A[p/\perp]$ ) gilt.

## Beweis.

Aufgrund der NNF implizieren beide Bedingungen für jedes  $\varphi \in \mathbb{B}^A$

$$\hat{\varphi}(A[p/\perp]) \leq \hat{\varphi}(A[p/\top]) \quad \left( \text{bzw. } \hat{\varphi}(A[p/\top]) \leq \hat{\varphi}(A[p/\perp]) \right)$$

Damit folgt aus der Nichterfüllbarkeit von  $\hat{\varphi}[A/\top]$  (bzw.  $\hat{\varphi}[A/\perp]$ ) auch die von  $\hat{\varphi}[A/\perp]$  (bzw.  $\hat{\varphi}[A/\top]$ ) und somit die von  $A$ . □

Erfüllt  $A \in \text{NNF}$  eine der obigen Bedingung, kann ein Ast des „Wahrheitsbaums“ eliminiert werden. **Terminologie:** **Unit-** bzw. **Pure Literal-**Regel. Parallele Anwendungen für mehrere Atome sind erlaubt!

# Regel-baserte Definition von Davis-Putnam; Heuristik

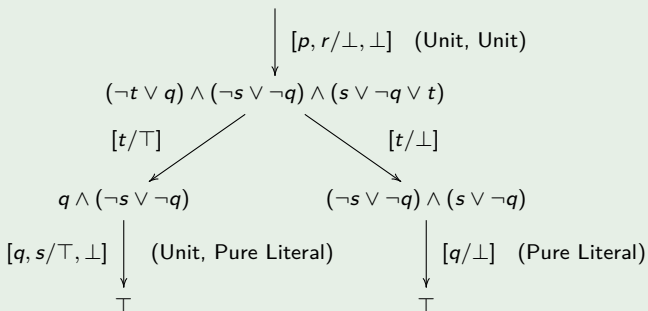
Unit- und Pure Literal-Regel sind so früh wie möglich anzuwenden.

Greift keine von beiden, resultiert zwingend eine binäre Verzweigung im „Wahrheitsbaum“; man spricht dann von der **Splitting**-Regel. Hier ist der „Preis“ für den Prozess der Auswahl des nächsten Atoms abzuwägen gegen die zu erwartende Vereinfachung beim restlichen Verfahren, z.B.

- ▷ das erste vorkommende Atom (keine Auswahlkosten);
- ▷ ein am häufigsten vorkommendes Atom;
- ▷ ein Atom  $p$ , für das die Gesamtlänge der Klauseln, in denen  $p$  vorkommt, also  $\sum_{p \in K_i} |K_i|$ , minimal ist;
- ▷ ein Atom  $p$ , das in den „kurzen“ Klauseln am häufigsten vorkommt; (braucht eine explizite Schranke, ab wann eine Klausel als „kurz“ gilt);
- ▷ ein Atom, bei dem die Differenz zwischen positiven und negativen Auftreten in den „kurzen“ Klauseln maximal ist.

## Beispiel

$$A = \neg p \wedge (\neg t \vee q \vee p) \wedge (\neg s \vee \neg q) \wedge (s \vee \neg q \vee t) \wedge (r \vee \neg p) \wedge \neg r$$



Während das Davis-Putnam-Verfahren auf beliebige Formeln in NNF anwendbar ist, sollten bei KNF-Eingaben die Vereinfachungen auf Folie [Folie 170](#), also das Entfernen subsumierter oder tautologischer Klauseln, nicht vergessen werden!

# Resolutionslemma

## Satz

Für alle Formeln  $A, B, C$  gilt  $\{A \vee B, \neg B \vee C\} \models A \vee C$ .

## Beweis.

Die Behauptung ist äquivalent zu  $\{\neg A \rightarrow B, B \rightarrow C\} \models \neg A \rightarrow C$  und damit auch zu  $\{\neg A \rightarrow B, B \rightarrow C\} \vdash \neg A \rightarrow C$ :

- |    |  |         |
|----|--|---------|
| 0. | $\neg A \rightarrow B$   | Ann.    |
| 1. | $B \rightarrow C$  | Ann.    |
| 2. | $\left[ \begin{array}{l} \neg A \\ B \\ C \end{array} \right.$ | Ann.    |
| 3. |  | MP, 2,0 |
| 4. |  | MP, 3,1 |
| 5. | $\neg A \rightarrow C$   | DT, 2-4 |



Dies liefert die Basis für den folgenden **Resolventen-Kalkül**:

# Resolution für Klauseln in Mengenschreibweise

## Definition

Das deduktive System  $\mathcal{R}$  auf der Menge  $\mathcal{C}$  aller Klauseln hat nur die Regel

$$\frac{K + \{\ell\} \quad \{\neg\ell\} + M}{K \cup M} \quad \text{mit der Resolvente } K \cup M$$

für Klauseln  $K$ ,  $M$  und ein Literal  $\ell$ , das nicht in  $K$ , und dessen Negation nicht in  $M$  vorkommt („+“ steht für disjunkte Vereinigung).

Eine  $\mathcal{R}$ -Herleitung einer Klausel  $K$  aus  $F \in \text{KNF}$ , geschrieben  $F \vdash_{\text{res}} K$ , ist eine Klausel-Folge  $\langle K_i : i \leq n \rangle$  mit  $K_n = K$  und

- ▷ für  $k < n$  gilt entweder  $K_k \in F$ , oder  $K_k$  ist Resolvente von  $K_i$  und  $K_j$  mit  $i, j < k$ .

Beachte die Ähnlichkeit der Resolventen-Regel mit der Schnittregel des Sequenzen-Kalküls unter Berücksichtigung von  $(\neg R)$ , wobei  $\Gamma_0 = \Gamma_1 = \emptyset$ .

# Aussagenlogik versus Klausel-Logik

In Analogie zur bisherigen Aussagenlogik erhalten wir nun eine „Klausel-Logik“ mit folgenden Entsprechungen:

	Aussagenlogik	Klausel-Logik
Grundbausteine	Formeln $A \in \mathcal{F}[\mathcal{A}]$	Klauseln $K$
Prämissenmengen	$\Gamma \subseteq \mathcal{F}[\mathcal{A}]$ , potentiell unendlich	Formeln $F \in \text{KNF}$ , endlich
Folgerung	$\Gamma \models A$	$F \models_{\text{res}} K$ , gleichbedeutend mit $F \models K$
Herleitung	$\Gamma \vdash A$ , $\Gamma \vdash A$ , etc.	$F \vdash_{\text{res}} K$

Fasst man  $F \in \text{KNF}$  als Menge von Klauseln auf, kann man für beliebiges  $A \in \mathcal{F}[\mathcal{A}]$  fragen, ob in der Aussagenlogik  $F \models A$  gilt. Falls  $A$  keine Klausel ist, gibt es dafür keine Entsprechung in der Klausel-Logik.

Trotzdem wird auch die Klausel-Logik die Unerfüllbarkeit von  $F \cup \{\neg A\}$  mittels einer Herleitung  $F \cup \text{KNF}(\neg A) \vdash_{\text{res}} \emptyset$  nachweisen können (s.u.).



## Satz

Der  $\mathcal{R}$ -Kalkül ist korrekt aber *nicht vollständig*, d.h.,

$F \vdash_{\text{res}} K$  impliziert  $F \models_{\text{res}} K$  aber nicht notwendig umgekehrt

Zudem kann  $F \models A \in \text{KNF}$  gelten, wobei  $A$  mindestens zwei Klauseln hat.

## Beweis.

Das Resolutionslemma impliziert Korrektheit. Umgekehrt verträgt sich Subsumption mit  $\models_{\text{res}}$  aber nicht mit  $\vdash_{\text{res}}$ : Zwar gilt

$$\{\{p, q\}, \{p, \neg q\}\} \models_{\text{res}} \{p\} \quad \text{und} \quad \{\{p, q\}, \{p, \neg q\}\} \vdash_{\text{res}} \{p\}$$

Aber  $\{p\} \subseteq \{p, r\}$  impliziert nur  $\{\{p, q\}, \{p, \neg q\}\} \models_{\text{res}} \{p, r\}$ . Des Weiteren gilt  $\{p \vee q, p \vee \neg q, \neg p \vee q\} \models p \wedge q$ , was keine Klausel ist.  $\square$

## Satz (Widerlegungsvollständigkeit und Korrektheit, John Alan Robinson)

$F \in \text{KNF}$  ist genau dann unerfüllbar, wenn  $F \vdash_{\text{res}} \emptyset$ .

## Beweis.

Aus  $F \vdash_{\text{res}} \emptyset$  folgt  $F \vdash_{\text{res}} \ell$  und  $F \vdash_{\text{res}} \neg \ell$  für ein Literal  $\ell$ , nach obigem Satz also auch  $F \models \ell$  und  $F \models \neg \ell$ . Damit ist die Menge  $F$  unerfüllbar.

Sei  $F$  unerfüllbar. Betrachte die Anzahl  $k$  verschiedener Literale in  $F$ .

$k = 0$ : Dann gilt  $F = \emptyset$ .

**Annahme:** Die Behauptung stimmt für alle  $i < k$ .

$k > 0$ : OBdA enthalte  $F$  keine tautologischen oder subsumierten Klauseln. In  $F$  tritt ein Atom  $p$  positiv und negativ auf, sonst wäre  $F$  erfüllbar.

$F_+$  enthalte alle  $F$ -Klauseln, in denen  $p$  auftritt;

$F_-$  enthalte alle  $F$ -Klauseln, in denen  $\neg p$  auftritt;

$F_0$  enthalte alle  $F$ -Klauseln, in denen weder  $p$  noch  $\neg p$  auftritt.

Wegen  $F = F_+ \cup F_- \cup F_0$  folgt aus der Unerfüllbarkeit einer oder der Vereinigung zweier dieser Klauselmengen nach Annahme die Behauptung.

## Beweis, Fortsetzung.

Sind  $F_+ \cup F_0$ ,  $F_- \cup F_0$  und  $F_+ \cup F_-$  erfüllbar, so zeigen wir:

$$F_+ \cup F_0 \vdash_{\text{res}} p \quad \text{und} \quad F_- \cup F_0 \vdash_{\text{res}} \neg p$$

Zwecks Elimination von  $p$  aus  $F_+$  setze  $F_{\oplus} := \{K - \{p\} : K \in F_+\}$ .

Wäre  $F_{\oplus} \cup F_0$  erfüllbar, dann gäbe es  $\varphi \in (F_{\oplus} \cup F_0)^{\mathcal{D}}$  mit  $\varphi(p) = 0$ , also würde  $F_+ \cup F_0$  wie auch  $F_- \cup F_0$  und somit  $F$  von  $\varphi$  erfüllt,  $\perp$ .

Also gilt  $F_{\oplus} \cup F_0 \vdash_{\text{res}} \emptyset$ , etwa mittels einer  $\mathcal{R}$ -Herleitung  $\langle J_i : i < n \rangle$  **minimaler Länge**. Da  $F_0$  nach Voraussetzung erfüllbar ist, muss für jede Resolvente  $J_k$  von Klauseln  $J_i$  und  $J_j$  mit  $i, j < k$ , gelten  $F_0 \not\vdash_{\text{res}} J_i$  oder  $F_0 \not\vdash_{\text{res}} J_j$ ; andernfalls wäre  $J_k$  überflüssig. Damit liefert

$$J'_i := \begin{cases} J_i \cup \{p\} & \text{falls } F_0 \not\vdash_{\text{res}} J_i \\ J_i & \text{sonst} \end{cases}$$

eine  $\mathcal{R}$ -Herleitung von  $p$  aus  $F_+ \cup F_0$ . Analog gilt  $F_- \cup F_0 \vdash_{\text{res}} \neg p$ . Beides zusammen impliziert  $F \vdash_{\text{res}} \emptyset$ . □

# Resolutions-Heuristiken

## Definition

Für  $A \in \text{KNF}$  bezeichnet  $\mathbf{Res}(A)$  die Menge aller Klauseln, die in endlich vielen Schritten als Resolventen aus den Klauseln von  $A$  konstruierbar sind.

Ein naiver Algorithmus basiert auf der Tatsache, dass  $A \in \text{KNF}$  genau dann erfüllbar ist, wenn  $\emptyset \in \mathbf{Res}(A)$  gilt. Dies wird nicht empfohlen.

Stattdessen kann man sich auf **starke Herleitungen** beschränken, in denen

- ▷ keine Klausel mehrfach auftritt;
- ▷ keine tautologischen Klauseln auftreten;
- ▷ einmal subsumierte Klauseln nicht weiter verwendet werden.

Dies erlaubt es, aus  $\mathbf{Res}(A)$  bestimmte Klauseln zu entfernen und mit einer potentiell kleineren Menge  $\widetilde{\mathbf{Res}}(A)$  zu arbeiten.

Zur Handrechnung ziehen wir ein systematisches graphisches Verfahren vor.

## Beispiel (Die finanziellen Probleme der Familie Z, vergl. Folie 11)

Zunächst wandeln wir die Prämissen und die negierte(!) Schlußfolgerung in KNF um:

$$B_0 = \neg p \rightarrow \neg(q \wedge r \wedge s) \quad \Leftrightarrow p \vee \neg q \vee \neg r \vee \neg s \quad = \{p, \neg q, \neg r, \neg s\}$$

$$B_1 = q \quad = \{q\}$$

$$B_2 = r \vee s \quad = \{r, s\}$$

$$B_3 = t \rightarrow \neg r \quad \Leftrightarrow \neg t \vee \neg r \quad = \{\neg r, \neg t\}$$

$$B_4 = \neg t \rightarrow s \quad \Leftrightarrow t \vee s \quad = \{s, t\}$$

$$\neg A = \neg(\neg p \rightarrow (\neg r \wedge s)) \quad \Leftrightarrow \neg p \wedge (r \vee \neg s) \quad = \{\neg p\}, \{r, \neg s\}$$

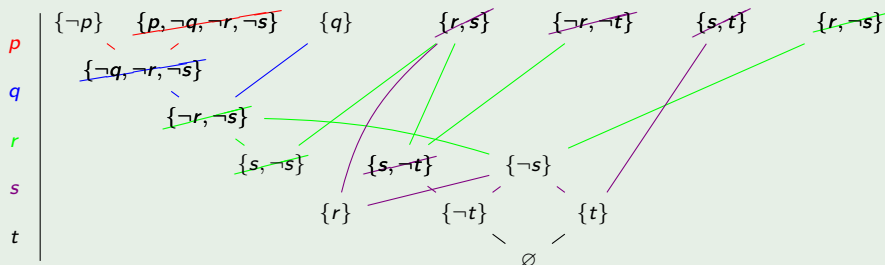
Die resultierende Klauselmenge

$$G = \{\{\neg p\}, \{p, \neg q, \neg r, \neg s\}, \{q\}, \{r, s\}, \{\neg r, \neg t\}, \{s, t\}, \{r, \neg s\}\}$$

kann nun in einem einfachen graphischen Verfahren auf (Un-)Erfüllbarkeit untersucht werden:

## Beispiel

- ▷ Ordne die auftretenden Klauseln horizontal an;
- ▷ Ordne die auftretenden Atome (beliebig) vertikal an;
- ▷ konstruiere **schichtweise** alle Resolventen bzgl. des aktuellen Atoms; streiche tautologische oder subsumierte Formeln sofort;



Das Streichen der verbliebenen nichtleeren Klauseln kann unterbleiben.

$\mathcal{R}$ -Herleitung:  $\{\neg p\}, \{p, \neg q, \neg r, \neg s\}, \{\neg q, \neg r, \neg s\}, \{q\}, \{\neg r, \neg s\}, \{r, \neg s\}, \{r, s\}, \{\neg r, \neg t\}, \{s, t\}, \{s, \neg t\}, \{\neg s\}, \{t\}, \{\neg t\}, \emptyset$ .

Zur Übung möge man eine andere Reihenfolge der Atome ausprobieren!

## Bemerkungen

- ▶ Das Berechnen des Resolutionsabschlusses  $Res(A)$  (außer tautologischen Klauseln) ist unter dem Namen **Stufenstrategie** bekannt. Sofern  $\emptyset$  nicht auftritt kann man sämtliche erfüllenden Belegungen bestimmen. (Für Handrechnung zu fehleranfällig.)
- ▶ Bei der sog. **Stützmengenrestriktion** werden Unit-Klauseln bevorzugt zur Resolventenbildung herangezogen.
- ▶ Bei **P-** bzw. **N-Resolution** sollte eine der beteiligten Klauseln nur positive (negative) Literale enthalten.
- ▶ Zumindest für Formeln in 2-KNF und für Horn-Formeln (mit höchstens einem positiven Literal pro Klausel) ist die Resolventen-Methode effizient. I.A. ist das leider nicht der Fall:

# Resolution ist i.A. nicht effizient

## Satz

Es gibt eine Folge  $\emptyset \neq A_k \in \text{KNF}$ ,  $k \in \mathbb{N}$ , mit folgenden Eigenschaften:

- ▷ in  $A_k$  kommen höchstens die Atome  $p_i$ ,  $i < 2k + 1$  vor;
- ▷  $A_k$  hat  $k + 1$  Klauseln;
- ▷ keine der  $2^{k+1} - 1$  Klauseln in  $\text{Res}(A_k)$  subsumiert eine andere.

## Beweis.

$k = 0$ :  $A_0 = p_0$  hat  $2^1 - 1 = 1$  Resolventen.

**Annahme:**  $A_k = \bigwedge_{i < k+1} K_{k,i}$  habe die gewünschten Eigenschaften.

$k + 1$ :  $A_{k+1} := \text{KNF}(A_k \vee p_{2k+1}) \wedge (\neg p_{2k+1} \vee p_{2k+2})$  hat zwei Atome und eine Klausel mehr als  $A_k$ , und  $\text{Res}(A_{k+1})$  hat alle um  $p_{2k+1}$  bzw.  $p_{2k+2}$  vergrößerten Resolventen von  $A_k$ , sowie  $\{\neg p_{2k+1}, p_{2k+2}\}$ . Dabei entstehen keine neuen Mengeninklusionen zwischen Klauseln.  $\square$



# Erfüllbarkeitsäquivalenz

Die Frage, ob  $\Gamma \models A$  gilt, ist für endliche Mengen  $\Gamma$  äquivalent zur Frage, ob  $B := \bigwedge \Gamma \wedge \neg A$  nicht erfüllbar ist. Selbst wenn alle Prämissen in  $\Gamma$  und  $A$  in KNF vorliegen, ist das für  $B$  i.A. nicht der Fall, und wie auf [Folie 171](#) gesehen, kann die Umwandlung von  $B$  zu einer äquivalenten Formel  $C \in \text{KNF}$  zu exponentiellem Längenwachstum führen.

Stattdessen kann man versuchen, eine kürzere KNF-Formel  $D$  zu finden, die genau dann erfüllbar ist, wenn dies für  $B$  gilt, und dann deren Erfüllbarkeit mit einem passenden Algorithmus zu überprüfen.

## Definition

Formeln  $B, D \in \mathcal{F}[A]$  heißen **erfüllbarkeitsäquivalent** ( $B \models_e D$ , engl. **equi-satisfiable**), falls  $B$  genau dann erfüllbar ist, wenn dies für  $D$  gilt.

Wegen  $p \models_e q$  für  $p \neq q$  ist  $\models$  echt in  $\models_e$  enthalten.

# Die Tseitin-Transformation - Idee

Laut G. S. Tseitin<sup>12</sup> lassen sich Formeln aus  $\mathcal{F}[\mathcal{A}]$  erfüllbarkeitsäquivalent so in KNF umwandeln, dass die Länge nur linear wächst.

**Idee:** ordne gewissen Teilformeln  $B$  von  $A$  (vergl. Folie 48, keine Literale) ein frisches Atom  $p$  zu und bilde die Konjunktion aller (leicht zu bestimmenden!) Formeln  $\text{KNF}(p \leftrightarrow B)$ ,  $B$  geeignete Teilformel von  $A$ :

$B$	$p \leftrightarrow B$	$\text{KNF}(p \leftrightarrow B)$ in Mengendarstellung
$\neg C$	$(\neg C \rightarrow p) \wedge (p \rightarrow \neg C)$	$\{C, p\}, \{\neg p, \neg C\}$
$C \wedge D$	$(C \wedge D \rightarrow p) \wedge (p \rightarrow C \wedge D)$	$\{\neg C, \neg D, p\}, \{\neg p, C\}, \{\neg p, D\}$
$C \vee D$	$(C \vee D \rightarrow p) \wedge (p \rightarrow C \vee D)$	$\{\neg C, p\}, \{\neg D, p\}, \{\neg p, C, D\}$
$C \rightarrow D$	$(\neg C \vee D \rightarrow p) \wedge (p \rightarrow \neg C \vee D)$	$\{C, p\}, \{\neg D, p\}, \{\neg p, \neg C, D\}$
$C \leftrightarrow D$	$((\neg C \vee D) \wedge (\neg D \vee C) \rightarrow p) \wedge (p \rightarrow (\neg C \vee D) \wedge (\neg D \vee C))$	$\{C, D, p\}, \{\neg C, \neg D, p\}, \{\neg p, \neg C, D\}, \{\neg p, C, \neg D\}$
$C \oplus D$	$((C \wedge \neg D) \vee (D \vee \neg C) \rightarrow p) \wedge (p \rightarrow (C \vee \neg D) \vee (D \vee \neg C))$	$\{C, \neg D, p\}, \{\neg C, D, p\}, \{\neg p, C, D\}, \{\neg p, \neg C, \neg D\}$

<sup>12</sup> On the complexity of derivation in propositional calculus, Leningrad Seminar on Mathematic Logic, September 1966

# Die Tseitin-Transformation - Vorbereitung: Top-Level

Wie üblich werden doppelte Negationen sofort eliminiert.

- ▶ Falls  $A = \neg C$  kann für  $C = D \star E$  mit  $\star \in \{\wedge, \vee, \rightarrow\}$  die Negation mittels de Morgan bzw. Umschreiben direkt eliminiert werden. Für  $C = D \leftrightarrow E$  wurde oben explizit das **exklusive Oder**  $\oplus$  als Negation eingeführt. Spätere Negationen liefern negative Literale, somit ist die erste Regel überflüssig!
- ▶ Im Fall  $A = C \wedge D$  (und nur dann) kann man die Transformation separat auf  $C$  und  $D$  anwenden. Speziell für  $A = C \leftrightarrow D$  soll daher  $(C \rightarrow D) \wedge (D \rightarrow C)$ , oder besser  $(\neg C \vee D) \wedge (\neg D \vee C)$  bearbeitet werden.
- ▶  $A = C \vee D$  bleibt unverändert, während  $A = C \rightarrow D$  zu  $\neg C \vee D$  umgeschrieben wird.
- ▶  $A = C \oplus D$  wird ersetzt durch  $(C \wedge \neg D) \vee (D \wedge \neg C)$ .

# Die Tseitin-Transformation - Umsetzung

Nun sei  $A$  oBdA eine Disjunktion  $A = A' \vee A''$ .

- ▷ Ordne den **echten binären Teilformeln**  $B = C \star D$  von  $A$  ein frisches Atom  $p_B$  zu; das liefert die erste Klausel  $\{p_{A'}, p_{A''}\}$ ;
- ▷ bilde gemäß Tabelle  $\text{KNF}(p \leftrightarrow B')$ ; die binäre Verknüpfung  $B'$  zweier Literale entsteht durch Einsetzen der passenden Atome in  $C$  bzw.  $D$ ;
- ▷ bilde die Konjunktion  $\mathbf{Tse}(A)$  aller oben konstruierten Klauseln.

## Bemerkung

Drei oder mehr aufeinanderfolgende Kon- oder Disjunktionen können ebenso gehandhabt werden wie binäre: die KNF wächst nur um weitere Klauseln:

$$C \wedge D \wedge E \mapsto \{\neg C, \neg D, \neg E, p\}, \{C, \neg p\}, \{D, \neg p\}, \{E, \neg p\}$$

$$C \vee D \vee E \mapsto \{\neg C, p\}, \{\neg D, p\}, \{\neg E, p\}, \{\neg p, C, D, E\}$$

# Die Tseitin-Transformation - Beispiele

Beispiel ( $A = (\neg s \wedge p) \leftrightarrow ((q \rightarrow r) \vee \neg p)$ )

Der rechtzeitige Übergang zur BNF spart weitere Klauseln:

$$\left( (\neg s \wedge p) \rightarrow ((q \rightarrow r) \vee \neg p) \right) \wedge \left( ((q \rightarrow r) \vee \neg p) \rightarrow (\neg s \wedge p) \right)$$

$$(\neg(\neg s \wedge p) \vee (\neg q \vee r \vee \neg p)) \wedge (\neg(\neg q \vee r \vee \neg p) \vee (\neg s \wedge p))$$

$$(\neg t_0 \vee t_1) \wedge (\neg t_1 \vee t_0) : \{\neg t_0, t_1\}, \{\neg t_1, t_0\}$$

$$t_0 \leftrightarrow (\neg s \wedge p) : \{s, \neg p, t_0\}, \{\neg t_0, \neg s\}, \{\neg t_0, p\}$$

$$t_1 \leftrightarrow (\neg q \vee r \vee \neg p) : \{q, t_1\}, \{\neg r, t_1\}, \{p, t_1\}, \{\neg t_1, \neg q, r, \neg p\}$$

**$Tse(A)$**  besteht dann aus allen blauen Klauseln.

## Beispiel (Hauptjunktoren $\vee$ statt $\wedge$ )

$$(\neg(\neg s \wedge p) \wedge (\neg q \vee r \vee \neg p)) \vee (\neg(\neg q \vee r \vee \neg p) \vee (\neg s \wedge p)) = B$$

$$w_0 \vee w_1 : \{w_0, w_1\}$$

$$w_0 \leftrightarrow \neg t_0 \wedge t_1 : \{t_0, \neg t_1, w_0\} \{ \neg w_0, \neg t_0 \}, \{ \neg w_0, t_1 \}$$

$$w_1 \leftrightarrow \neg t_1 \wedge t_0 : \{t_1, \neg t_0, w_1\} \{ \neg w_1, \neg t_1 \} \{ \neg w_1, t_0 \}$$

$$t_0 \leftrightarrow (\neg s \wedge p) : \{s, \neg p, t_0\} \{ \neg t_0, \neg s \} \{ \neg t_0, p \}$$

$$t_1 \leftrightarrow (\neg q \vee r \vee \neg p) : \{q, t_1\} \{ \neg r, t_1 \} \{ p, t_1 \} \{ \neg t_1, \neg q, r, \neg p \}$$

$Tse(B)$  besteht dann aus allen **orangenen** und **blauen** Klauseln.

## Beispiel ( $A = (p \wedge \neg q) \vee \neg(r \wedge s)$ )

$$t_0 \vee t_1 : \{t_0, \neg t_1\}$$

$$t_0 \leftrightarrow p \wedge \neg q : \{ \neg p, q, t_0 \} \{ p, \neg t_0 \} \{ \neg q, \neg t_0 \}$$

$$t_1 \leftrightarrow r \wedge s : \{ \neg r, \neg s, t_1 \} \{ r, \neg t_1 \} \{ s, \neg t_1 \}$$

# Tseitin und Erfüllbarkeitsäquivalenz

Die Tseitin-Konstruktion motiviert folgende Halbordnung auf  $\mathcal{F}[\mathcal{A}]$ :

## Definition

Für  $A, B \in \mathcal{F}[\mathcal{A}]$  gilt  $B \sqsubseteq_t A$ , sofern folgende Bedingungen erfüllt sind:

- (T0)  $\mathcal{O}(A) \subseteq \mathcal{O}(B)$ ;
- (T1)  $\{B\}^\triangleright \subseteq \{A\}^\triangleright$  (oder  $B \sqsubseteq A$ , vergl. Lemma auf [Folie 67](#));
- (T2) zu jedem  $\varphi \in \{A\}^\triangleright$  stimmt ein  $\psi \in \{B\}^\triangleright$  auf  $\mathcal{O}(A)$  mit  $\varphi$  überein.

Beachte: (T2) spezifiziert eine volle Relation  $\{A\}^\triangleright \twoheadrightarrow \{B\}^\triangleright$ .

## Satz

- (a)  $\sqsubseteq_e$  ist die transitive Hülle von  $\sqsubseteq_t \cup \sqsubseteq_t^{\text{op}}$ .
- (b) Jedes  $A \in \mathcal{F}[\mathcal{A}]$  erfüllt  $\mathbf{Tse}(A) \sqsubseteq_t A$ , also auch  $A \sqsubseteq_e \mathbf{Tse}(A)$ .

## Beweis.

- (a) Sind  $A$  und  $B$  erfüllbar, so gilt  $A \sqsubseteq_t \top \sqsupseteq_t B$ , was  $\mathbb{H}_e \subseteq \sqsubseteq_t \cup (\sqsubseteq_t^{\text{op}})$  impliziert. Andererseits kann wegen (T1) nicht  $\top \sqsubseteq_t \perp$ , und wegen (T2) nicht  $\perp \sqsubseteq_t \top$  gelten. Aus  $\mathbb{H} \subseteq \mathbb{H}_e$  folgt Entsprechendes auch für eine widersprüchliche Formel  $A$  und eine erfüllbare Formel  $B$ .
- (b) Jede Formel  $A \in \mathcal{F}[\mathcal{A}]$  erfüllt  $\mathcal{O}(A) \subseteq \mathcal{O}(\mathbf{Tst}(A))$ . OBdA sei  $A \in \mathcal{F}[\mathcal{A}]$  eine Disjunktion.

Ein  $\psi \in \{\mathbf{Tst}(A)\}^\triangleright$  erfüllt alle Klauseln von  $\mathbf{Tst}(A)$ , speziell die erste. Rücksubstitution der echten binären Teilformeln von  $A$  für die frischen Atome in dieser Klausel (ohne Mengenschreibweise) rekonstruiert die Ausgangsformel  $A$ , also folgt  $\hat{\psi}(A) = 1$ .

Falls  $\varphi \in \{A\}^\triangleright$  setzen wir für jede verwendete Instanz  $p \leftrightarrow B'$

$$\psi(p) := \hat{\varphi}(B) \quad \text{und sonst} \quad \psi(q) = \varphi(q)$$

Dann gilt nach Konstruktion  $\hat{\psi}(\mathbf{Tst}(A)) = 1$ . □



# Teil 2

# Prädikatenlogik

(1. Stufe mit Gleichheit)

# Inhaltsverzeichnis, Teil 2

- 8 Motivation und Überblick
- 9 Syntax der Prädikatenlogik
- 10 Elementare Semantik der Prädikatenlogik
- 11 Skolem, Herbrand, Gödel
  - "Normalformen" und Skolemisierung
  - Allgemeingültigkeit: Herbrand und Gödel
  - Die Semi-Entscheidbarkeit des  $AGP(PL)$
  - Kompaktheit
- 12 Algorithmen
  - Tableaus in der PL
  - Resolution in der PL

# Kapitel 8

## Motivation und Überblick

# Defizite der Aussagenlogik

- ▷ Die Aussagenlogik (AL) ist überall anwendbar, wo potentiell wahre oder falsche Aussagen formuliert und miteinander kombiniert werden können, unabhängig vom Kontext.
- ▷ Sie ist weniger dafür geeignet zwischen verschiedenen Anwendungsbereichen zu unterscheiden, genauer: Aussagen über einzelne Elemente eines spezifischen (nichtleeren) Datenbereiches zu formulieren, **und ihr Verhältnis zueinander**, z.B. für natürlichen Zahlen, gerichtete Graphen oder Datenbanken. Ihre recht einfache mathematische Struktur ist Konsequenz dieser beschränkten Ausdrucksfähigkeit.

Man braucht somit eine Möglichkeit, **die atomaren Formeln an die Gegebenheiten der Datenbereiche von Interesse anzupassen**. Das, und noch etwas mehr, leistet die Prädikatenlogik 1. Stufe ( $PL_1$ ).

# Mögliche Anwendungen in der Informatik

Viele Anwendungen bedienen sich der  $PL_1$ , z.B.

- ▶ Lösung von Anfragen auf Datenmengen in der KI oder in Informationssystemen;
- ▶ Formulierung von Integritätsbedingungen auf Daten; etwa Schleifeninvarianten eines Programms, Constraints auf XML-Dateien oder Datenbankeinträgen;
- ▶ Lösung von Constraint-Systemen beim Testen oder Planen.
- ▶ Logisches Programmieren, z.B. in PROLOG.

# Syntax, Übersicht

Frege<sup>13</sup> definierte 1879 die Syntax der  $PL_1$  in seiner „[Begriffsschrift](#)“ – Eine der arithmetischen nachgebildete Formelsprache des reinen Denkens“.

In moderner Terminologie:

- ▷ Eine **Signatur**  $Fun + Pred \xrightarrow{S} \mathbb{N}$  weist **Operatoren** und **Prädikaten** (d.h., formalen Funktions- bzw. Relationssymbolen) eine Stelligkeit zu;
- ▷ eine (abzählbare) Menge  $\mathcal{V}$  von **Variablen** liefert in einem 1. Schritt die **Fun**-Algebra  $Term(Fun, \mathcal{V})$ , einen abstrakten Datenbereich aus **Termen** in den Operatoren (für den der [Rekursionssatz](#) gilt!);
- ▷ Prädikate und **formale Gleichheit**  $\doteq$  mit Termen als Argumenten bilden nun die dem Datenbereich angepaßte **atomare Formelmeng**e  $\mathcal{A}(S)$ ;
- ▷ die bekannten Junktoren der Aussagenlogik und **neue unäre Junktoren**  $\forall x$  („für alle  $x$ “) und  $\exists x$  („es gibt ein  $x$ “) für jede Variable  $x$ , liefern die Menge **FO**( $S$ ) aller Formeln;  $\forall$  und  $\exists$  heißen **Quantoren**.

<sup>13</sup> Friedrich Ludwig Gottlob Frege (1848–1925)

# Semantik, Übersicht

Tarskis<sup>14</sup> Semantik von 1934 in moderner Terminologie:

- ▷ **S-Strukturen**  $\mathcal{M} = \langle D, I \rangle$  interpretieren  $\mathcal{S}$  in einer **Trägermenge**  $D$ ; speziell ist  $I(R) \subseteq D^{S(R)}$  für  $R \in \mathbf{Pred}$  eine  $\mathcal{S}(R)$ -stellige Relation;
- ▷ Jede **Belegung**  $\mathcal{V} \xrightarrow{\sigma} D$  der Variablen liefert einen eindeutigen **Fun**-Homomorphismus  $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\check{\sigma}} \langle D, I_{\mathbf{Fun}} \rangle$ ;
- ▷ Alle atomaren Formeln (in den Symbolen von  $\mathbf{Pred}$  und  $\dot{=}$ ) liefern gemäß  $\check{\sigma}$  und  $I_{\mathbf{Pred}}$  **überprüfbare Aussagen bzgl.  $\mathcal{M}$** , und damit einen Wahrheitswert; analog zu  $\mathcal{A} \xrightarrow{\varphi} \mathbb{B}$  der AL.
- ▷ Solch eine Belegung  $\mathcal{A}(\mathcal{S}) \xrightarrow{\bar{\sigma}} \mathbb{B}$  setzt sich eindeutig zu einer Bewertung  $\hat{\sigma}$  aller Formeln  $F \in \mathbf{FO}(\mathcal{S})$  fort, analog zu  $\mathcal{F}[\mathcal{A}] \xrightarrow{\hat{\varphi}} \mathbb{B}$ .
- ▷ Mit einem fiesem Trick lassen sich die Semantiken für Terme und Formeln in eine ähnliche Form bringen.

<sup>14</sup> Alfred Tarski bzw. ursprünglich Alfred Tarski, 1901 – 1983

# Beschreibung mathematischer Beziehungen

## Beispiel

**Syntax:** Konstanten  $1, 2, 3$ ; 2-stellige Funktionssymbole  $+, /$ ;  
2-stelliges Prädikat  $<$ :

$$\text{Signatur } \mathcal{S} = \langle \{1_{/0}, 2_{/0}, 3_{/0}, +_{/2}, /_{/2}\}, \{<_{/2}\} \rangle$$

Terme (Infix)  $1, 1 + (2/3), (x + 3)/2, \dots$

**Logik:** Junktoren  $\rightarrow, \wedge$ , Quantoren  $\forall, \exists$ ;

Formeln  $x < 3, \forall x \forall y (x < y \rightarrow \exists z (x < z \wedge z < y))$

**Semantik:** Datenbereich  $D = \mathbb{Q}$ , Konstante  $1$  bis Prädikat  $<$  mit der üblichen Bedeutung.

**Achtung:** Andere Interpretationen der Signatur  $\mathcal{S}$  sind möglich und dürfen nicht ignoriert werden!



# Beschreibung von Beziehungen zwischen Daten

## Beispiel

**Syntax:** ein Operator  $WeiteDerReise(-) /_1$ ,  
 drei Prädikate  $istHund(-) /_1$ ,  $istFisch(-) /_1$ ,  $< /_2$

**Logik:** Junktoren  $\rightarrow$ ,  $\wedge$ , Quantor  $\forall$ ;

typische Formel:

$$\forall x \forall y (istHund(x) \wedge istFisch(y) \rightarrow WeiteDerReise(x) < WeiteDerReise(y))$$

**Semantik:** Datenbereich  $D = \{Lassie, Nemo\} \cup \mathbb{N} \cup \{\perp\}$

Die Standard-Interpretation der Funktion  $WeiteDerReise(-)$  liefert die Weite der Reise, die das Tier im Argument zurückgelegt hat, oder  $\perp$  sonst.

$istHund$  und  $istFisch$  möge die charakteristische Funktion von  $\{Lassie\}$  bzw.  $\{Nemo\}$  sein.

# Kapitel 9

## Syntax der Prädikatenlogik

# Syntax der Prädikatenlogik, Details

Auf zwei **entscheidbaren** abzählbaren Mengen **Fun** und **Pred**, möglichst disjunkt zum Alphabet der AL, betrachten wir eine **Signatur**

$$\mathbf{Fun} + \mathbf{Pred} \xrightarrow{\mathcal{S}} \mathbb{N}$$

Die **Fun**-Elemente dienen als **Operatoren** oder Funktionssymbole (wie zuvor), und die **Pred**-Elemente als **Prädikate** oder Relationssymbole (neu).

Üblicherweise verwenden wir Kleinbuchstaben  $f, g, h \dots$  für erstere, und Großbuchstaben  $R, S, T \dots$  für letztere.

$f_{/k}$  und  $R_{/k}$  ist eine Kurzschreibweise für  $\mathcal{S}(f) = k$  bzw.  $\mathcal{S}(R) = k$ .

**Achtung:** Ein weiteres binäres Prädikat  $\doteq_{/2} \notin \mathbf{Pred}$  spielt später in der Semantik eine Sonderrolle als **formale Gleichheit**.

0-stellige Operatoren/Prädikate heißen **Konstanten/Propositionen**.

Weiter sei  $\mathcal{V}$  eine (abzählbare entscheidbare) Menge von **Variablen**.

# Aufbau der Formeln in drei Schritten

- ▷ Zuerst bilden wir die **Termalgebra**  $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ ;

$$t ::= v \mid f(t_0, \dots, t_{S(f)-1}) \quad \text{mit } v \in \mathcal{V} \quad \text{und } f \in \mathbf{Fun}$$

- ▷ Aus den Termen bilden wir  $\mathbf{AT} := \mathbf{Atm}(\mathbf{Pred} + \{\dot{=}\}, \mathbf{Term}(\mathbf{Fun}, \mathcal{V}))$ , die Menge der **atomaren Formeln** (mit Gleichheit):

$$A ::= t_0 \dot{=} t_1 \mid R(t_0, \dots, t_{S(R)-1}) \quad \text{mit } R \in \mathbf{Pred}$$

Damit ist  $\mathbf{AT}$  eine disjunkte Vereinigung  $\sum_{R \in \mathbf{Pred} + \{\dot{=}\}} \mathbf{AT}_R$ .

- ▷ Und schließlich bilden wir mit Hilfe der um  $\forall x/1$  und  $\exists x/1$ ,  $x \in \mathcal{V}$ , erweiterten Junktormenge  $\mathcal{J}_Q$  die **Termalgebra**  $\mathbf{FO}(\mathcal{S})$  der **prädikatenlogischen Formeln erster Stufe** (**first order formulae**):

$$F ::= A \mid \top \mid \perp \mid \neg F \mid (F_0 \star F_1) \mid (\forall x F) \mid (\exists x F)$$

mit  $A \in \mathbf{AT}$ ,  $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$  und  $x \in \mathcal{V}$ .

# Gebundene und freie Variablen

Als einstellige Junktoren binden  $\forall x$  und  $\exists x$  stärker als alle 2-stelligen.

## Definition

Die Menge  $\mathbf{V}(t)$  der in einem Term  $t$  **auf tretenden** Variablen ist

$$\mathbf{V}(x) = \{x\} \quad \text{und} \quad \mathbf{V}(f(t_0, \dots, t_{S(f)-1})) = \bigcup \{ \mathbf{V}(t_i) : i < S(f) \}$$

Analog sind die in einer (atomaren) Formel auftretenden Variablen definiert.

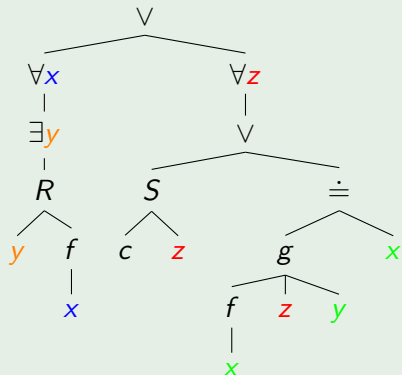
In  $(Qx F)$  ist  $F$  der **Geltungsbereich** für  $Qx$ ; jedes Vorkommen von  $x$  in einem solchen Geltungsbereich heißt **gebunden**, außerhalb jedes solchen Geltungsbereichs **frei**. Die Menge der **gebunden/frei vorkommenden Variablen** in  $H \in \mathbf{FO}(S)$  wird mit **GV(H)** bzw. **FV(H)** bezeichnet; sie brauchen nicht disjunkt zu sein!

Formeln ohne frei vorkommende Variablen heißen **abgeschlossen**.

Formeln der  $PL_1$  als 2-stufige Syntaxbäume

In der Baumdarstellung dienen die Prädikate sowie  $\doteq$  als Schnittstellen zwischen den Bäumen der Terme und dem logischen Syntax-Baum.

Beispiel  $( (\forall x \exists y R(y, f(x))) \vee \forall z (S(c, z) \vee g(f(x), z, y) \doteq x) )$



Oberhalb der **frei** vorkommenden Variablen findet sich kein mit dieser Variablen verbundener Quantor. Dagegen sind die Vorkommen  $x$ ,  $y$  und  $z$  gebunden.

# Anmerkungen

Der Begriff der **Entscheidbarkeit** einer Menge wird erst in TheoInf2 offiziell eingeführt. Informell soll er hier bedeuten, dass wir ihre Elemente effizient, d.h., mit geringem Rechenaufwand oder sogar unmittelbar erkennen können.

## Lemma

- ▷ *Die Entscheidbarkeit der Signatur  $\mathcal{S}$  und der Variablenmenge  $\mathcal{V}$  vererbt sich auf die Mengen der Terme und der (atomaren) Formeln.*
- ▷ *Zusammengesetzte Terme und Formeln lassen sich eindeutig zerlegen.*
- ▷ *Gebundene und freie Vorkommen von Variablen lassen sich effizient bestimmen.*

# Kapitel 10

## Elementare Semantik der Prädikatenlogik



# $\mathcal{S}$ -Strukturen

Das Ziel ist oft die Beschreibung von Beziehungen zwischen Elementen eines nichtleeren **konkreten** strukturierten Datenbereichs  $D$ .

Dafür war eine passende Signatur  $\mathcal{S} = \mathbf{Fun} + \mathbf{Pred}$  gewählt worden, evtl. mit suggestiven Namen für die Funktionen- bzw. Relationsymbole.

Eine Semantik für  $\mathbf{FO}(\mathcal{S})$  muss berücksichtigen, dass **andere** Interpretationen von  $\mathcal{S}$  auf  $D$  wie auch **andere** Datenbereiche  $D'$  existieren können.

## Definition

Unter einer  **$\mathcal{S}$ -Struktur**  $\mathcal{M} = \langle D, I \rangle$  versteht man eine Menge  $D \neq \emptyset$ , den **Datenbereich**, zusammen mit einer **Interpretation** der Symbole aus  $\mathcal{S}$  in  $D$

$$D^{\mathcal{S}(f)} \xrightarrow{I(f)} D \text{ für } f \in \mathbf{Fun} \quad \text{und} \quad D^{\mathcal{S}(R)} \xrightarrow{I(R)} \mathbb{B} \text{ für } R \in \mathbf{Pred}$$

Außerdem soll immer  $I(\doteq) = \mathbf{id}_D$  gelten (dies rechtfertigt die Bezeichnung „formale Gleichheit“). Schreibweise:  $f^{\mathcal{M}}$  und  $R^{\mathcal{M}}$  statt  $I(f)$  bzw.  $I(R)$ .

Belegungen, Semantik der Terme für festes  $\mathcal{M} = \langle D, I \rangle$ 

In der AL konnte die Menge  $\mathcal{A}$  der atomaren Formeln direkt mit Wahrheitswerten belegt werden. In der  $PL_1$  gelingt das nur indirekt. Dennoch wollen wir hier versuchen möglichst viel von der AL zu übernehmen.

## Definition

Eine **Belegung der Variablen** ist eine Abbildung  $\mathcal{V} \xrightarrow{\sigma} D$  bzw.  $\sigma \in D^{\mathcal{V}}$ ; gelegentliche Schreibweise  $\sigma \in \mathcal{M}^{\mathcal{V}}$  (zwecks Erinnerung an  $I$ ).

Aufgrund des [Rekursionssatzes](#) lässt sich solch eine Belegung  $\sigma$  eindeutig zu einem **Fun**-Homomorphismus  $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\check{\sigma}} \langle D, I_{\mathbf{Fun}} \rangle$  fortsetzen, der **Semantik der Terme bzgl.  $\sigma \in \mathcal{M}^{\mathcal{V}}$** .

Das liefert auf **kanonische Weise** die **Semantik der atomaren Formeln bzgl.  $\sigma$**  als Abbildung  $\mathbf{AT} = \mathbf{Atm}(\mathbf{Pred} + \{\dot{=}\}, \mathbf{Term}(\mathbf{Fun}, \mathcal{V})) \xrightarrow{\bar{\sigma}} \mathbb{B}$ , die auf verschiedene Weisen beschrieben werden kann:

Semantik atomarer Formeln für festes  $\mathcal{M}$ 

Für jedes Prädikat  $R \in \mathbf{Pred} + \{\dot{=}\}$  ist die Menge  $\mathbf{AT}_R$  der atomaren Formeln, in denen  $R$  auftritt, isomorph zu  $\mathbf{Term}^{S(R)}$ : man entfernt einfach das Symbol  $R$ , bzw. fügt es wieder hinzu. Nun lässt sich  $\mathbf{AT} = \sum_{R \in \mathbf{Pred} + \{\dot{=}\}} \mathbf{AT}_R \xrightarrow{\bar{\sigma}} \mathbb{B}$  mittels **Fallunterscheidung** definieren:

$$\begin{array}{ccc}
 \mathbf{Term}^{S(R)} & \xrightarrow{\check{\sigma}^{S(R)}} & D^{S(R)} \\
 \uparrow \text{strip}_R & & \downarrow R^{\mathcal{M}} \\
 \mathbf{AT}_R & \xrightarrow{\bar{\sigma}_R} & \mathbb{B}
 \end{array}$$

Oder mittels Teilmengen  $R^{\mathcal{M}}$  anstelle von charakteristischen Funktionen:

$$\bar{\sigma}(t_0 \dot{=} t_1) = 1 \text{ gdw } \check{\sigma}(t_0) = \check{\sigma}(t_1)$$

$$\bar{\sigma}(R(t_0, \dots, t_{S(R)-1})) = 1 \text{ gdw } \langle \check{\sigma}(t_0), \dots, \check{\sigma}(t_{S(R)-1}) \rangle \in R^{\mathcal{M}} \subseteq D^{S(R)}$$

Semantik allgemeiner Formeln für festes  $\mathcal{M}$ 

Schließlich können wir den Rekursionssatz ein weiteres Mal anwenden und  $\mathbf{AT} \xrightarrow{\bar{\sigma}} \mathbb{B}$  eindeutig zu einem Homomorphismus  $\mathbf{FO}(S) \xrightarrow{\hat{\sigma}} \mathbb{B}$  bzgl. der Signatur  $\mathcal{J}_Q$  fortsetzen, indem wir die Junktoren in  $\mathcal{J}$  analog zur AL Folie 20 behandeln. Die neuen Junktoren erfordern einen Zwischenschritt:

## Definition

Jedes Paar  $\langle x, d \rangle \in \mathcal{V} \times D$  liefert eine **Modifikation**  $D^{\mathcal{V}} \xrightarrow{\{x/d\}} D^{\mathcal{V}}$ :

$$\sigma \mapsto \sigma\{x/d\}^a, \quad y \mapsto \begin{cases} d & \text{falls } y = x \\ \sigma(y) & \text{sonst} \end{cases}$$

Damit lässt sich die **Semantik quantifizierter Formeln** formulieren:

$$\hat{\sigma}(\forall x A) := \inf \{ \widehat{\sigma\{x/d\}}(A) : d \in D \}$$

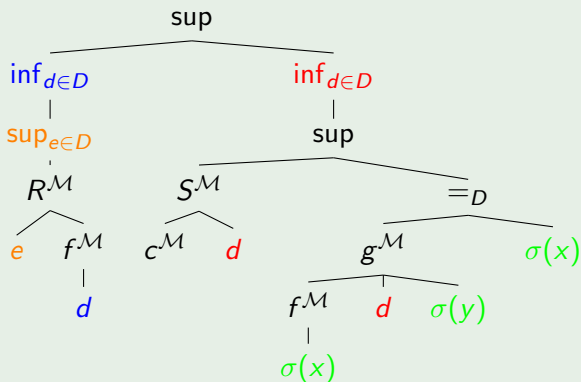
$$\hat{\sigma}(\exists x A) := \sup \{ \widehat{\sigma\{x/d\}}(A) : d \in D \}$$

<sup>a</sup> Beachte die Reihenfolge! Die Funktion steht hier rechts.

# Auswertung von Formeln in Baumform

Wir illustrieren die Auswertung einer Formel anhand des Beispiels auf  
 Folie 212 für eine  $\mathcal{S}$ -Struktur  $\mathcal{M} = \langle D, I \rangle$  und eine Belegung  $\sigma \in D^{\mathcal{V}}$ :

Beispiel  $(\hat{\sigma}(\forall x \exists y R(y, f(x))) \vee \forall z (S(c, z) \vee g(f(x), z, y) \doteq x))$



## Beispiel (Modellierung eines konkreten Problems)

Eine Frau, die ein Porträt betrachtet, sagt: „Geschwister habe ich keine. Und die Mutter dieser Frau ist meiner Mutter Tochter.“ Wer ist da abgebildet?

Wir führen Konstanten  $a_{/0}$  und  $b_{/0}$  für die abgebildete Frau bzw. die Beobachterin ein. Weiter benötigen wir ein zweistelliges Geschwister-Prädikat  $G_{/2}$ , um die erste Aussage formulieren zu können:

$$\forall y. \neg G(b, y) \quad (1)$$

Analog könnte man ein Tochter-Prädikat  $T$ , oder auch ein Mutter-Prädikat  $M$  einführen. Es gibt aber eine bessere Lösung: eine einstellige Mutter-Operation  $m_{/1}$ . Das erlaubt die Formalisierung der zweiten Aussage mittels einer formalen Gleichung:

$$m(m(a)) \doteq m(b) \quad (2)$$

Das liefert die Signatur  $\mathcal{S} = \mathbf{Fun} + \mathbf{Pred} = \{a_{/0}, b_{/0}, m_{/1}\} + \{G_{/2}\}$ .

## Beispiel (Fortsetzung)

Die intendierte  $\mathcal{S}$ -Struktur  $\mathcal{M}$  besteht aus der Menge  $D$  aller Menschen, mit zwei ausgewählten Frauen  $a^{\mathcal{M}}$  und  $b^{\mathcal{M}}$ , der Mutter-Funktion  $D \xrightarrow{m^{\mathcal{M}}} D$  und der Geschwister-Relation  $G^{\mathcal{M}} \subseteq D \times D$ .

Allgemein bekannte Tatsache über  $\mathcal{M}$ : Menschen ohne Geschwister sind die einzigen Kinder ihrer Mütter:

$$\forall y. \neg G(z, y) \rightarrow \forall u. (m(u) \doteq m(z) \rightarrow u \doteq z) \quad (3)$$

Was folgt aus den Prämissen (1), (2) und (3)? Modus Ponens mit (1) und der Instantiierung von (3) mit  $z = b$  ergibt

$$\forall u. (m(u) \doteq m(b) \rightarrow u \doteq b) \quad (4)$$

was für  $u = m(a)$  mit Modus Ponens aufgrund von (2) die Antwort liefert:

$$m(a) \doteq b$$

## Beispiel (Graphentheorie)

Die Theorie **gerichteter Graphen** benötigt nur ein zweistelliges Prädikat  $R_{/2}$  und keine Operatoren. In diesem Fall gilt

- ▶ **Term**(**Fun**,  $\mathcal{V}$ ) = **Term**( $\emptyset$ ,  $\mathcal{V}$ ) =  $\mathcal{V}$ , also immer  $\check{\sigma} = \sigma \in D^{\mathcal{V}}$ ;
- ▶ **AT** =  $\{ R(x, y) : x, y \in \mathcal{V} \}$ ;
- ▶  $\bar{\sigma}(R(x, y)) \in \mathbb{B}$  bestimmt, ob es eine **gerichtete** Kante von  $\sigma(x)$  nach  $\sigma(y)$  gibt ( $\bar{\sigma}(R(x, y)) = 1$ ), oder nicht ( $\bar{\sigma}(R(x, y)) = 0$ ).

**Schleifen** (engl. "loops"), also Kanten von einem Knoten zu sich selbst, sind a priori erlaubt. Man kann mittels mit  $\forall x. \neg R(x, x)$  eliminieren.

$$\forall x \forall y. (R(x, y) \wedge R(y, x) \rightarrow x \doteq y)$$

charakterisiert **gerichteten Graphen ohne 2-Zyklen**. Für **ungerichtete Graphen** muss  $R^{\mathcal{M}}$  symmetrisch sein: zwei entgegengesetzte gerichtete Kanten  $\bar{\sigma}(x) \rightleftarrows \bar{\sigma}y$  fasst man als ungerichtete Kante  $\bar{\sigma}(x) \text{ --- } \bar{\sigma}(y)$  auf.

$$\forall x \forall y. (R(x, y) \rightarrow R(y, x))$$



Andere Sicht auf die Semantik der Terme/Formeln,  $\mathcal{M}$  fest

Wir haben die Semantik der Terme/Formeln als durch Belegungen  $\sigma \in \mathcal{M}^{\mathcal{V}}$  parametrisierte Familien von Funktionen eingeführt:

$$D^{\mathcal{V}} \xrightarrow{(\check{\cdot})} D^{\mathbf{Term}(\mathbf{Fun}, \mathcal{V})} \quad , \quad \sigma \mapsto \check{\sigma}$$

$$D^{\mathcal{V}} \xrightarrow{(\hat{\cdot})} \mathbb{B}^{\mathbf{FO}(\mathcal{S})} \quad , \quad \sigma \mapsto \hat{\sigma}$$

Uncurrying<sup>15</sup> macht daraus 2-stellige (Auswertungs-)Funktionen

$$\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \times D^{\mathcal{V}} \xrightarrow{\mathcal{M}[\![\cdot]\!](-)} D, \quad \langle t, \sigma \rangle \mapsto \check{\sigma}(t)$$

$$\mathbf{FO}(\mathcal{S}) \times D^{\mathcal{V}} \xrightarrow{\mathcal{M}[\![\cdot]\!](-)} \mathbb{B}, \quad \langle A, \sigma \rangle \mapsto \hat{\sigma}(A)$$

Die zweite entspricht der Auswertung  $\mathcal{F}[\mathcal{A}] \times \mathbb{B}^{\mathcal{A}} \xrightarrow{E} \mathbb{B}$  der AL ► Folie 53.

Die Wahl desselben Namens für beide Funktionen spiegelt deren strukturelle Ähnlichkeit wider; die sog. **Semantik-Klammern**  $\llbracket \cdot \rrbracket$  sind **kontext-sensitiv!** Sie entstammen der **denotationellen Semantik** (Scott, Strachey 1971), und sind neben der formalen Semantik auch in der formalen Linguistik verbreitet.

<sup>15</sup> nach Haskell Brooks Curry (1900-1982)

# Fieser Trick

Aufgrund der Symmetrie des cartesischen Produkts erhalten wir mittels **currying** weitere durch Terme/Formeln parametrisierte Familien

$$\begin{aligned} \mathbf{Term}(\mathbf{Fun}, \mathcal{V}) &\xrightarrow{\mathcal{M}[\cdot]} D^{(D^{\mathcal{V}})} , t \mapsto \mathcal{M}[[t]] , \sigma \mapsto \mathcal{M}[[t]](\sigma) := \check{\sigma}(t) \\ \mathbf{FO}(S) &\xrightarrow{\mathcal{M}[\cdot]} \mathbb{B}^{(D^{\mathcal{V}})} , A \mapsto \mathcal{M}[[A]] , \sigma \mapsto \mathcal{M}[[A]](\sigma) = \hat{\sigma}(A) \end{aligned}$$

die ebenfalls **Semantik der Terme/Formeln** genannt werden!

[Der notationelle Aufwand erscheint disproportional hoch, und die Analogie zur AL wie wir sie eingeführt haben geht hier leider verloren. Dort mit der **dualen Erfüllungsrelation**  $\mathbf{E}^{\text{op}} \subseteq \mathbb{B}^{\mathcal{A}} \times \mathcal{F}[\mathcal{A}]$  zu arbeiten hätte zu einer durch Formeln parametrisierten Familie führen können, etwa

$$\mathcal{F}(\mathcal{A}) \xrightarrow{[\cdot]} \mathbb{B}^{(\mathbb{B}^{\mathcal{A}})} , A \mapsto [[A]] , \varphi \mapsto [[A]](\varphi) = \hat{\varphi}(A)$$

Ob die AL damit leichter verständlich gewesen wäre, sei dahingestellt.]

Man muss obige in der Literatur verbreitete Notation aber beherrschen! Ggf. geben wir die einfachere Variante in **orange** an und nutzen sie in Beweisen.

## $\mathcal{M}$ als Parameter

Bisher haben wir mit einer festen  $\mathcal{S}$ -Struktur  $\mathcal{M}$  gearbeitet. Das erlaubt uns Begriffe weitgehend parallel zur AL auch für die  $PL_1$  einzuführen.

Lässt man  $\mathcal{M}$  zu variieren, erhält man die **Familie** der durch die möglichen  $\mathcal{S}$ -Strukturen  $\mathcal{M}$  **indizierten** Auswertungsfunktionen

$$\mathbf{FO}(\mathcal{S}) \times D^\forall \xrightarrow{\mathcal{M}\llbracket - \rrbracket(-)} \mathbb{B} \quad \text{bzw.} \quad \mathbf{E}_{\mathcal{M}} \subseteq \mathbf{FO}(\mathcal{S}) \times D^\forall,$$

die zugehörigen Erfüllungsrelationen, wobei  $D$  von  $\mathcal{M}$  abhängt. Ein **Erfüller** von  $A \in \mathbf{FO}(\mathcal{S})$  ist somit ein **Paar**  $\langle \mathcal{M}, \sigma \in \mathcal{M}^\forall \rangle$ , während  $\sigma$  allein nur ein **Erfüller in  $\mathcal{M}$**  ist.

Die **Hüllenoperatoren** auf  $\mathbf{FO}(\mathcal{S})$  bezeichnen wir mit  $(\ )_{\mathcal{M}}^{\triangleleft} := \mathbf{E}_{\mathcal{M}}^{\triangleleft} \circ \mathbf{E}_{\mathcal{M}}^{\triangleright}$ , und ihren **Durchschnitt** mit  $(\ )^{\triangleright\triangleleft}$ . Auch damit kann man weitgehend analog zur AL verfahren, die dortigen Beweise lassen sich oft übernehmen.

Allerdings gibt es **keine Zerlegung der Form**  $(\ )^{\triangleright\triangleleft} := \mathbf{E}^{\triangleleft} \circ \mathbf{E}^{\triangleright}$  mehr! Beweise sind für generisches  $\mathcal{M}$  zu führen.

# Logische Folgerung, Erfüllbar- und Allgemeingültigkeit

## Definition (vergl. ▶ Folie 57)

Betrachte  $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$  (aus sog. **Prämissen**) und  $A, B \in \mathbf{FO}(\mathcal{S})$ .

- ▶ Falls  $A \in \Gamma^{\forall} \quad (A \in \Gamma_{\mathcal{M}}^{\forall})$ , d.h., jeder Erfüller der Prämissen (in  $\mathcal{M}$ ) erfüllt (in  $\mathcal{M}$ ) auch  $A$ , schreibt man  $\Gamma \models A$  ( $\Gamma \models_{\mathcal{M}} A$ ) und sagt „ $A$  **folgt (in  $\mathcal{M}$ ) logisch aus  $\Gamma$** “, d.h.,  $\models := (\bigcap_{\mathcal{M}} \models_{\mathcal{M}})$ ;
- ▶ Ist  $A$  geschlossen (die Belegung der Variablen also irrelevant), so nennt man  $\mathcal{M}$  **ein Modell** für  $A$ , sofern  $\models_{\mathcal{M}} A$  gilt;
- ▶ heißt  $A$  **allgemeingültig** oder **Tautologie**, falls  $\models A$  gilt;
- ▶  $B \in \mathbf{FO}(\mathcal{S})$  ( $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$ ) heißt **erfüllbar**, wenn eine  $\mathcal{S}$ -Struktur  $\mathcal{M} = \langle D, I \rangle$  existiert mit  $\{B\}_{\mathcal{M}}^{\exists} \neq \emptyset$  (bzw.  $\Gamma_{\mathcal{M}}^{\exists} \neq \emptyset$ ).

Wieder ist  $A$  genau dann allgemeingültig, wenn  $\neg A$  nicht erfüllbar ist.

Wir vermeiden in dieser VL Schreibweisen wie  $\mathcal{M}, \sigma \models A$  oder  $\mathcal{M} \models A$ , falls  $A$  geschlossen, um  $\mathcal{M}[[A]](\sigma) = \hat{\sigma}(A) = 1$  auszudrücken.

## Universeller und existentieller Abschluss

Im Folgenden werden wir oft an geschlossenen Formen (d.h., ohne freie Variablen) interessiert sein. Für jede Formel gibt es zwei kanonische Möglichkeiten, alle freien Variablen zu binden:

### Definition

Für  $A \in \mathbf{FO}(\mathcal{S})$  mit  $\mathbf{FV}(A) \subseteq \{x_i : i < n\}$  heißt

$$\forall x_0 \dots \forall x_{n-1} A \quad \text{bzw.} \quad \exists x_0 \dots \exists x_{n-1} A$$

**universeller** bzw. **existentieller Abschluss** von  $A$ .

### Lemma (HA!)

Für  $A \in \mathbf{FO}(\mathcal{S})$  mit  $\mathbf{FV}(A) \subseteq \{x_i : i < n\}$  sind jeweils äquivalent:

- ▷ die Allgemeingültigkeit von  $A$  und von  $\forall x_0 \dots \forall x_{n-1} A$ ;
- ▷ die Erfüllbarkeit von  $A$  und  $\exists x_0 \dots \exists x_{n-1} A$ . □

# Charakterisierung der Unerfüllbarkeit von Formelmengen

Das folgende Ergebnis lässt sich nahezu analog zum entsprechenden Ergebnis der AL beweisen, vergl. [Folie 58](#), lediglich für (2), (3)  $\Rightarrow$  (0) muss man auf ein allgemeines  $\mathcal{M}$  zurückgreifen.

## Lemma

Folgende Bedingungen sind für  $\Gamma \subseteq \mathbf{FO}(S)$  äquivalent:

- (0)  $\Gamma$  ist unerfüllbar, bzw.  $\Gamma_{\mathcal{M}}^{\triangleright} = \emptyset$  für alle  $S$ -Strukturen  $\mathcal{M}$ .
- (1)  $\Gamma \models A$  für alle Formeln  $A$ , bzw.  $\Gamma^{\triangleright\triangleleft} = \mathbf{FO}(S)$ .
- (2)  $\Gamma \models \perp$  bzw.  $\perp \in \Gamma^{\triangleright\triangleleft}$ .
- (3)  $\Gamma \models B$  und  $\Gamma \models \neg B$  bzw.  $\{B, \neg B\} \subseteq \Gamma^{\triangleright\triangleleft}$  für ein  $B \in \mathbf{FO}(S)$ .  $\square$

Das semantische Deduktionstheorem (sDT) der  $PL_1$ 

Lemma (sDT; Prämissen lassen sich zwischen  $\models$  und  $\rightarrow$  verschieben)

Für  $\Gamma \subseteq \mathbf{FO}(S) \ni A, B$  gilt:  $\Gamma \cup \{A\} \models B$  gdw.  $\Gamma \models A \rightarrow B$ .

Beweis.

( $\Rightarrow$ ): Die Belegung  $\sigma \in D^\forall$  für eine  $S$ -Struktur  $\mathcal{M} = \langle D, I \rangle$  erfülle  $\Gamma$ .  
 $\mathcal{M}[A](\sigma) = \hat{\sigma}(A) = 1$  impliziert nach Annahme  $\mathcal{M}[B](\sigma) = \hat{\sigma}(B) = 1$ ;  
 andernfalls gilt  $\mathcal{M}[A](\sigma) = \hat{\sigma}(A) = 0 \leq \mathcal{M}[B](\sigma) = \hat{\sigma}(B)$ .  
 In beiden Fällen ergibt sich  $\mathcal{M}[A \rightarrow B](\sigma) = \hat{\sigma}(A \rightarrow B) = 1$ .

( $\Leftarrow$ ): Für  $\mathcal{M} = \langle D, I \rangle$  erfüllt  $\sigma \in \mathbf{E}_{\mathcal{M}}^\forall(\Gamma \cup \{A\}) = \mathbf{E}_{\mathcal{M}}^\forall(\Gamma) \cap \mathbf{E}_{\mathcal{M}}^\forall(\{A\})$   
 sowohl  $\Gamma$  als auch  $A$ , nach Annahme also auch  $A \rightarrow B$ , und wegen  
 $\mathcal{M}[A](\sigma) = \hat{\sigma}(A) \leq \mathcal{M}[B](\sigma) = \hat{\sigma}(B)$  ebenfalls  $B$ . □

Korollar

$\{A, A \rightarrow B\} \models B$  bzw.  $\Gamma \cup \{A\}$  unerfüllbar gdw.  $\Gamma \models \neg A$ . □

# Modus Ponens, Modus Tollens und Kontraposition

Die aus den deduktiven Systemen der AL bekannten Typen von Schlussfolgerungen und Ähnliche gelten natürlich auch in der Semantik sowohl der AL als auch der  $PL_1$ :

## Satz

Betrachte  $\Gamma \subseteq \mathbf{FO}(S) \ni A, B$ .

- ▷  $\Gamma \models B$  und  $\Gamma \models B \rightarrow A$  impliziert  $\Gamma \models A$  (*Modus Ponens*).
- ▷  $\Gamma \models B \rightarrow A$  und  $\Gamma \models \neg A$  impliziert  $\Gamma \models \neg B$  (*Modus Tollens*).
- ▷  $\Gamma \models B \rightarrow A$  und  $\Gamma \models A$  impliziert *i.A. nicht*  $\Gamma \models B$  (*Modus Bogus*).
- ▷  $\Gamma \cup \{B\} \models \neg A$  gdw.  $\Gamma \cup \{A\} \models \neg B$  (*Kontraposition*).

## Beweis.

HA. □



Die kanonische Halbordnung und Äquivalenz auf  $\mathbf{FO}(S)$ 

## Definition

Für eine  $S$ -Struktur  $\mathcal{M} = \langle D, I \rangle$  und jede Belegung  $\sigma \in D^{\mathcal{V}}$  induziert  $\mathbf{FO}(S) \xrightarrow{\hat{\sigma}} \mathbb{B}$  eine Quasiordnung  $\sqsubseteq_{\mathcal{M}, \sigma}$  auf  $\mathbf{FO}(S)$ ;  $\sqsubseteq_{\mathcal{M}}$  bezeichnet analog zur AL den Durchschnitt über alle  $\sigma \in \mathcal{M}^{\mathcal{V}}$ , und  $\sqsubseteq$  den Durchschnitt aller  $\sqsubseteq_{\mathcal{M}}$ ,  $\mathcal{M}$  eine  $S$ -Struktur.

Wie gewohnt bezeichnen wir die resultierenden ÄR'n mit  $\vDash_{\mathcal{M}}$  bzw.  $\vDash$ .

## Lemma

Für  $A, B \in \mathbf{FO}(S)$  und eine  $S$ -Struktur  $\mathcal{M}$  sind äquivalent:

- ①  $B \sqsubseteq_{\mathcal{M}} A$
- ②  $\{B\} \vDash_{\mathcal{M}} A$
- ③  $\{B\}_{\mathcal{M}}^{\triangleright} \subseteq \{A\}_{\mathcal{M}}^{\triangleright}$
- ④  $\mathcal{M} \llbracket B \rightarrow A \rrbracket(\sigma) = \hat{\sigma}(B \rightarrow A) = 1$  für alle  $\sigma \in D^{\mathcal{V}}$

Weiter gilt natürlich auch  $B \sqsubseteq A$  gdw.  $\{B\} \vDash A$ . □

## Freie Variablen – das Koinzidenzlemma

In der AL konnte die Bewertung  $\hat{\varphi}(B)$  einer Formel  $B$  nur von den Werten  $\varphi(p)$  derjenigen Atome  $p$  abhängen, die in  $B$  vorkommen.

Entsprechend kann in der  $PL_1$  die Semantik  $\mathcal{M}\llbracket A \rrbracket(\sigma) = \hat{\sigma}(A)$  nur von den Werten der in  $A$  auftretenden atomaren Formeln abhängen, und somit nur von den  $\sigma$ -Werten der in diesen vorkommenden Variablen.

Gebundene Auftreten von Variablen nehmen dabei keinen Einfluss; daher können gebundene Variablen auch umbenannt werden (vergl. [Folie 237](#)):

### Lemma (Koinzidenzlemma)

*Ist  $A$  eine  $PL_1$ -Formel über der Signatur  $\mathcal{S}$  und  $\mathcal{M} = \langle D, I \rangle$  eine  $\mathcal{S}$ -Struktur, so gilt für alle Belegungen  $\sigma, \tau \in \mathcal{M}^V$  mit  $\sigma(x) = \tau(x)$  für alle  $x \in \mathbf{FV}(A)$ :*

$$\mathcal{M}\llbracket A \rrbracket(\sigma) = \mathcal{M}\llbracket A \rrbracket(\tau) \quad \text{bzw.} \quad \hat{\sigma}(A) = \hat{\tau}(A) \quad \square$$

# Rechenregeln für Quantoren

Neben den Rechenregeln auf [Folie 71](#) und [Folie 72](#) gelten weitere Regeln für die mittels Quantoren gebildeten neuen unären Junktoren  $\forall x$  und  $\exists x$ :

Lemma (weitere logische Äquivalenzen in  $\mathbf{FO}(\mathcal{S})$ )

$$\neg \forall x. A \equiv \exists x. \neg A \qquad \neg \exists x. A \equiv \forall x. \neg A \qquad (1)$$

$$\forall x. A \wedge \forall x. B \equiv \forall x. (A \wedge B) \qquad \exists x. A \vee \exists x. B \equiv \exists x. (A \vee B) \qquad (2)$$

$$\forall x \forall y. A \equiv \forall y \forall x. A \qquad \exists x \exists y. A \equiv \exists y \exists x. A \qquad (3)$$

(1) *verallgemeinert De Morgan*. Sofern  $x \notin \mathbf{FV}(A)$  gilt weiterhin

$$A \star Qx B \equiv Qx (A \star B) \quad \text{für } Q \text{ Quantor und } \star \in \{\wedge, \vee, \rightarrow\} \qquad (4)$$

$$Qx B \rightarrow A \equiv \bar{Q}x (B \rightarrow A) \quad \text{für } Q \text{ und } \bar{Q} \text{ komplementär} \qquad (5)$$

Aber i.A.

$$\forall x A \vee \forall x B \not\equiv \forall x (A \vee B) \qquad \exists x A \wedge \exists x B \not\equiv \exists x (A \wedge B) \qquad \forall x \exists y A \not\equiv \exists y \forall x A$$

## Beispiel

Betrachte die Signatur  $\mathcal{S} = \{0_{/0}, 1_{/0}, +_{/2}\} + \{\leq_{/2}\}$  und die  $\mathcal{S}$ -Struktur  $\mathbb{N}$  mit der üblichen Interpretation der Operatoren und des Prädikats.

$$(a) \quad \forall x. \exists y. (x + 1 \leq y) \quad \text{bzw.} \quad (b) \quad \exists y. \forall x. (x + 1 \leq y)$$

bedeutet, dass es (a) zu jeder Zahl eine echt größere gibt (korrekt), bzw. dass es (b) eine größte Zahl gibt (falsch).

1-stellige Prädikate, die gerade bzw. ungerade Zahlen charakterisieren,

$$G(x) := \exists y. (y + y \doteq x) \quad \text{sowie} \quad U(x) := \exists y. (y + y \doteq x + 1)$$

erlauben es ausdrücken, dass (c) alle Zahlen gerade oder ungerade sind (korrekt), und dass (d) alle Zahlen gerade sind, oder alle Zahlen ungerade sind (falsch), formal

$$(c) \quad \forall x. (G(x) \vee U(x)) \quad \text{bzw.} \quad (d) \quad \forall x. G(x) \vee \forall x. U(x)$$

# Substitutionen via Rekursionsatz und Modifikationen

► Folie 218 definierte die Modifikation einer Belegung  $\sigma \in \mathcal{M}^{\mathcal{V}}$  durch Paare  $\langle x, d \rangle \in \mathcal{V} \times D$ . Betrachte speziell den Fall  $D = \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ :

## Definition

Für das Bild  $\mathcal{V} \xrightarrow{\vartheta} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$  der Inklusion  $\mathcal{V} \xrightarrow{\iota} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$  unter endlich vielen Modifikationen

$$(\mathbf{Term}(\mathbf{Fun}, \mathcal{V}))^{\mathcal{V}} \xrightarrow{\{x_i/t_i\}} (\mathbf{Term}(\mathbf{Fun}, \mathcal{V}))^{\mathcal{V}} \quad i < k$$

bezeichnet man die eindeutigen Fortsetzungen

- $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) \xrightarrow{\check{\vartheta}} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$
- $\mathbf{AT} \xrightarrow{\bar{\vartheta}} \mathbf{AT}$
- $\mathbf{FO}(\mathcal{S}) \xrightarrow{\hat{\vartheta}} \mathbf{FO}(\mathcal{S})$

als **Substitution** auf Termen, bzw. (atomaren) Formeln. Insbesondere ist  $\vartheta$  eine Belegung, die an nur endlich vielen Stellen von der Identität abweicht.

## Anwendung von Substitutionen

Wendet man Substitutionen **von rechts** an, braucht man  $\check{\vartheta}$ ,  $\bar{\vartheta}$  und  $\hat{\vartheta}$  nicht länger zu unterscheiden. **Achtung:** Sie binden stärker als Junktoren!

Bei der Anwendung auf quantifizierte Formeln dürfen aber keine neuen Bindungen erzeugt werden. Ggf. sind gebundene Variable umzubenennen:

### Definition (Vereinheitlichte Substitutionen)

$$x\vartheta := \check{\vartheta}(x)$$

$$f(t_0, \dots, t_{S(f)-1})\vartheta := f(t_0\vartheta, \dots, t_{S(f)-1}\vartheta)$$

$$(t_0 \doteq t_1)\vartheta := t_0\vartheta \doteq t_1\vartheta$$

$$R(t_0, \dots, t_{S(R)-1})\vartheta := R(t_0\vartheta, \dots, t_{S(R)-1}\vartheta)$$

$$(\neg A)\vartheta := \neg(A\vartheta)$$

$$(A \star B)\vartheta := A\vartheta \star B\vartheta$$

$$(\mathcal{Q}x A)\vartheta := \mathcal{Q}y (A\{x/y\}\vartheta) \text{ mit } y = y\vartheta \notin \mathbf{V}(A)$$

( $\{x/y\}\vartheta$  ist natürlich die Komposition von Modifikationen, die erst  $\{x/y\}$  und dann  $\vartheta$  anwendet.)

## Substitutionslemma und gebundene Umbenennung

Der Zusammenhang zwischen Substitutionen (in Termen und (atomaren) Formeln) und der Modifikation von Belegungen nimmt nun folgende eindrucksvolle Form an, was sich mittels Induktion über den Aufbau von Termen bzw. Formeln zeigen lässt (gute Übung für die Notation!):

Substitutionslemma für Terme und Formeln  $\xi$ , Beweis umseitig

$$\mathcal{M}[\xi\{x/t\}](\sigma) = \mathcal{M}[\xi](\sigma\{x/\mathcal{M}[t](\sigma)\}) \quad \tilde{\sigma}(\xi\{x/t\}) = \sigma\{\widetilde{x/\tilde{\sigma}(t)}\}(\xi)$$

Korollar.

- ① Ist  $A \in \mathbf{FO}(\mathcal{S})$  allgemeingültig, dann auch  $A\{x/t\}$ .
- ② Die Formel  $\forall x A \rightarrow A\{x/t\}$  ist allgemeingültig.

Korollar (Gebundene Umbenennung erhält Äquivalenz).

$$\mathcal{Q}x A \vDash \mathcal{Q}y A\{x/y\} \text{ sofern } y \notin \mathbf{FV}(A). \quad \square$$

## Beweis des Substitutionslemmas

## Beweis für Terme.

Wir schreiben  $\mathbf{u}$  für  $\langle u_0, \dots, u_{n-1} \rangle \in \mathbf{Term}(\mathbf{Fun}, \mathcal{V})^n$ .

- ▷  $\xi$  ist eine von  $x$  verschiedene Variable  $u$ :

$$\mathcal{M}[\mathbf{u}\{x/t\}](\sigma) = \mathcal{M}[\mathbf{u}](\sigma) = \mathcal{M}[\mathbf{u}](\sigma\{x/\mathcal{M}[t](\sigma)\})$$

- ▷  $\xi = x$ :

$$\mathcal{M}[x\{x/t\}](\sigma) = \mathcal{M}[t](\sigma) = \mathcal{M}[x](\sigma\{x/\mathcal{M}[t](\sigma)\})$$

- ▷  $\xi = f(\mathbf{u})$ :

$$\begin{aligned} \mathcal{M}[f(\mathbf{u})\{x/t\}](\sigma) &= f^{\mathcal{M}}\langle \mathcal{M}[\mathbf{u}\{x/t\}](\sigma) \rangle \\ &= f^{\mathcal{M}}\langle \mathcal{M}[\mathbf{u}](\sigma\{x/\mathcal{M}[t](\sigma)\}) \rangle \\ &= \mathcal{M}[f(\mathbf{u})](\sigma\{x/\mathcal{M}[t](\sigma)\}) \end{aligned}$$



## Beweis für atomare Formeln

- ▷  $\xi$  ist eine Gleichung  $u_0 \doteq u_1$ :

$$\mathcal{M}[(u_0 \doteq u_1)\{x/t\}](\sigma) = 1$$

$$\text{gdw. } \mathcal{M}[u_0\{x/t\}](\sigma) = \mathcal{M}[u_1\{x/t\}](\sigma)$$

$$\text{gdw. } \mathcal{M}[u_0](\sigma\{x/\mathcal{M}[t](\sigma)\}) = \mathcal{M}[u_1](\sigma\{x/\mathcal{M}[t](\sigma)\})$$

$$\text{gdw. } \mathcal{M}[u_0 \doteq u_1](\sigma\{x/\mathcal{M}[t](\sigma)\}) = 1$$

- ▷  $\xi$  ist eine Prädikatauswertung  $P(\mathbf{u})$ :

$$\mathcal{M}[P(\mathbf{u})\{x/t\}](\sigma) = 1$$

$$\text{gdw. } \langle \mathcal{M}[\mathbf{u}\{x/t\}](\sigma) \rangle \in P^{\mathcal{M}}$$

$$\text{gdw. } \langle \mathcal{M}[\mathbf{u}](\sigma\{x/\mathcal{M}[t](\sigma)\}) \rangle \in P^{\mathcal{M}}$$

$$\text{gdw. } \mathcal{M}[P(\mathbf{u})](\sigma\{x/\mathcal{M}[t](\sigma)\}) = 1$$

## Beweis für aussagenlogisch zusammengesetzte Formeln

- ▷  $\xi$  ist eine Negation  $\neg B$ :

$$\begin{aligned} \mathcal{M}[\neg B\{x/t\}](\sigma) &= 1 - \mathcal{M}[B\{x/t\}](\sigma) \\ &= 1 - \mathcal{M}[B](\sigma\{x/\mathcal{M}[t](\sigma)\}) \\ &= \mathcal{M}[\neg B](\sigma\{x/\mathcal{M}[t](\sigma)\}) \end{aligned}$$

- ▷  $\xi$  ist eine Konjunktion  $B \wedge C$ :

$$\begin{aligned} \mathcal{M}[(B \wedge C)\{x/t\}](\sigma) &= \inf\{\mathcal{M}[B\{x/t\}](\sigma), \mathcal{M}[C\{x/t\}](\sigma)\} \\ &= \inf\left\{\mathcal{M}[B](\sigma\{x/\mathcal{M}[t](\sigma)\}), \right. \\ &\quad \left. \mathcal{M}[C](\sigma\{x/\mathcal{M}[t](\sigma)\})\right\} \\ &= \mathcal{M}[B \wedge C](\sigma\{x/\mathcal{M}[t](\sigma)\}) \end{aligned}$$

- ▷  $\xi$  ist eine Disjunktion  $B \vee C$ : analog, mit  $\sup$  anstelle von  $\inf$ .
- ▷  $\xi$  ist eine Implikation  $B \rightarrow C$ : umschreiben zu  $\neg B \vee C$ .

## Beweis für quantifizierte Formeln

- ▷  $\xi$  ist eine  $\forall$ -quantifizierte Formel  $\forall y B$ :

$$\begin{aligned}
 & \mathcal{M}[(\forall y. B)\{x/t\}](\sigma) \quad (\text{Achtung: } y \text{ könnte in } t \text{ auftreten!}) \\
 &= \mathcal{M}[\forall z. B\{y/z\}\{x/t\}](\sigma) \text{ mit } z \notin V(B) \cup \{x\} \cup V(t) \\
 &= \inf\{\mathcal{M}[B\{y/z\}\{x/t\}](\sigma\{z/d\}) : d \in D\} \\
 &= \inf\{\mathcal{M}[B\{y/z\}](\sigma\{z/d\}\{x/\mathcal{M}[t](\sigma\{z/d\})\}) : d \in D\} \\
 &= \inf\{\mathcal{M}[B\{y/z\}](\sigma\{z/d\}\{x/\mathcal{M}[t](\sigma)\}) : d \in D\} \text{ da } z \notin V(t) \\
 &= \inf\{\mathcal{M}[B\{y/z\}](\sigma\{x/\mathcal{M}[t](\sigma)\}\{z/d\}) : d \in D\} \text{ da } z \neq x \\
 &= \mathcal{M}[\forall z. B\{y/z\}](\sigma\{x/\mathcal{M}[t](\sigma)\}) \\
 &= \mathcal{M}[\forall y. B](\sigma\{x/\mathcal{M}[t](\sigma)\}) \text{ da } z \notin V(B)
 \end{aligned}$$

- ▷  $\xi$  ist eine  $\exists$ -quantifizierte Formel  $\exists y B$ : analog mit sup statt inf. □

# PL<sub>1</sub>-spezifische Folgerungen

## Satz

- 1 Falls  $x \notin \mathbf{FV}(\Gamma)$  für  $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$ , dann  $\Gamma \models A$  gdw.  $\Gamma \models \forall x A$  (*Generalisierung*);  
 – insbesondere  $\{A\} \models \forall x A$ , bzw.  $\models A \rightarrow \forall x A$ , sofern  $x \notin \mathbf{FV}(A)$ .
- 2 Entsteht  $A'$  aus  $A$  durch erlaubte (beachte Quantoren!) Ersetzung einiger (nicht notwendig aller) Vorkommen von  $x$  durch  $y$ , dann  $\models \forall x \forall y (x \doteq y \rightarrow (A \leftrightarrow A'))$  (*Variante der Kongruenz*)

## Beweis

- 1 Mit jedem Erfüller  $\langle \mathcal{M}, \sigma \in D^{\mathcal{V}} \rangle$  von  $\Gamma$  ist auch  $\langle \mathcal{M}, \sigma\{x/d\} \rangle$  mit  $d \in D$  ein solcher. Also folgt aus  $\Gamma \models A$  sofort  $\Gamma \models \forall x A$ . Umgekehrt genügt es, den Fall  $d = \sigma(x)$  zu betrachten.
- 2 HA! □

## Beispiele

Beispiel ( Falls  $x \in \mathbf{FV}(A)$  braucht  $\{A\} \models \forall x A$  nicht zu gelten.)

Für  $\mathcal{S} = \{R_{/1}\}$  und  $A = R(x)$  betrachte  $\mathcal{M} = \langle \{0, 1\}, R^{\mathcal{M}} = \{0\} \rangle$ .  
Die konstante 0-wertige Belegung  $\sigma \in \{0, 1\}^{\mathcal{V}}$  liefert

$$\mathcal{M} \llbracket A \rrbracket (\sigma) = \hat{\sigma}(A) = 1 \quad \text{aber} \quad \mathcal{M} \llbracket \forall x A \rrbracket (\sigma) = \hat{\sigma}(\forall x A) = 0$$

da auch  $\mathcal{M} \llbracket A \rrbracket (\sigma\{x/1\}) = \hat{\sigma}\{x/1\}(A) = 0$  im Infimum auftritt.

Beispiel (  $\{\forall x A\} \models A$  )

Wende DT mit  $t = x$  auf  $\forall x A \rightarrow A\{x/t\}$  an, was nach ▶ Folie 237  
allgemeingültig ist.

Beispiel (  $\models \exists x (R(x) \rightarrow \forall x R(x))$  )

Die Formel wird in  $\mathcal{M}$  mit 1 bewertet, wenn  $R^{\mathcal{M}}(d) = 0$  für ein, oder  
wenn  $R^{\mathcal{M}}(d) = 1$  für jedes  $d \in D$  gilt, also immer

## Lemma

$$\{\forall x(A \rightarrow B)\} \models \forall x A \rightarrow \forall x B$$

## Beweis.

	$\{\forall x A, \forall x (A \rightarrow B)\} \models \forall x B$	wegen DT zu zeigen
gdw.	$\{(\forall x A) \wedge \forall x (A \rightarrow B)\} \models \forall x B$	$\Gamma$ endlich
gdw.	$\{\forall x (A \wedge (A \rightarrow B))\} \models \forall x B$	nach Rechenregel (2)
gdw.	$\{\forall x (A \wedge (\neg A \vee B))\} \models \forall x B$	gemäß AL
gdw.	$\{\forall x ((A \wedge \neg A) \vee (A \wedge B))\} \models \forall x B$	Distributivität
gdw.	$\{\forall x (\perp \vee (A \wedge B))\} \models \forall x B$	gemäß AL
gdw.	$\{\forall x (A \wedge B)\} \models \forall x B$	$\perp$ neutral bzgl. $\vee$
gdw.	$\{(\forall x A) \wedge \forall x B\} \models \forall x B$	nach Rechenregel (2)
gdw.	$\{\forall x A, \forall x B\} \models \forall x B$	trivial und korrekt

## Lemma

$$\models \exists x \forall y A \rightarrow \forall y \exists x A$$

## Beweis.

	$\{\exists x \forall y A\} \models \forall y \exists x A$	wegen DT zu zeigen
gdw.	$\{\exists x \forall y A\} \models \exists x A$	Generalisierung
gdw.	$\{\neg \exists x A\} \models \neg \exists x \forall y A$	Kontraposition
gdw.	$\{\forall x \neg A\} \models \forall x \neg \forall y A$	de Morgan
gdw.	$\{\forall x \neg A\} \models \neg \forall y A$	Generalisierung
gdw.	$\{\forall x \neg A, \forall y A\} \models \perp$	Korollar zu DT
gdw.	$\{\exists y \forall x \neg A, \exists x \forall y A\} \models \perp$	existentieller Abschluß
gdw.	$\exists y \forall x \neg A \wedge \exists x \forall y A$ nicht erfüllbar	offensichtlich wahr <span style="float: right;">□</span>

Beispiel (  $\models \forall x \forall y (x \doteq y \rightarrow (f(x, y) = g(x) \leftrightarrow f(y, y) = g(x)))$  )

Dies gilt immer, wenn  $\mathcal{S}$  Funktionssymbole  $f_{/2}$  und  $g_{/1}$  enthält.

# Kapitel 11

## Skolem, Herbrand, Gödel



# Bereinigte Formeln

Die Syntax der  $PL_1$  enthält Fallstricke, die man explizit umgehen muss.

## Definition

$A \in \mathbf{FO}(\mathcal{S})$  heißt **bereinigt**, sofern

- ▶ keine Variable frei und gebunden auftritt, d.h.,  $\mathbf{FV}(A) \cap \mathbf{GV}(A) = \emptyset$ ;
- ▶ jede Variable höchstens einmal gebunden wird.

Durch iterierte gebundene Umbenennung lässt sich jede Formel bereinigen:

## Lemma

Zu jeder Formel  $A \in \mathbf{FO}(\mathcal{S})$  existiert eine bereinigte Formel  $B \in \mathbf{FO}(\mathcal{S})$  mit  $A \vDash B$ . □

Wie [Rechenregel \(2\)](#) für Quantoren zeigt, braucht die Konjunktion/Disjunktion bereinigter Formeln nicht mehr bereinigt zu sein. Ungeschicktes Bereinigen kann Formeln aber auch unnötig aufblähen (s.u.).

# Normalformen

Die [Motivation](#), Formeln der AL in bestimmte „Normalformen“ zu überführen, greift auch hier. Ziel sind einfachere Beweise und effizientere Algorithmen. Dabei werden wir überwiegend an geschlossenen Formeln interessiert sein.

Auf [Folie 227](#) haben wir bereits gesehen, wie Formeln durch **äußere Quantoren** sinnvoll in geschlossenen Formeln überführt werden können.

Wir betrachten nun zwei Typen von  $PL_1$ -Normalformen:

- ▷ **Pränex-Normalform**: alle Quantoren außen; diese erweisen sich als **logisch äquivalent** zur Ausgangsformel;
- ▷ **Skolem-Normalform**: PNF ohne Existenz-Quantor; diese sind i.A. nur **„erfüllbarkeitsäquivalent“** zur Ausgangsformel, wobei dieser Begriff ähnlich wie in der AL gefasst werden kann, siehe [Folie 256](#).

# Pränex- und Skolem<sup>16</sup> Normalform

## Definition

Ist  $B$  quantorenfrei, so nennt man eine Formel  $A \in \mathbf{FO}(S)$  der Form

$$Q_0 y_0 Q_1 y_1 \dots Q_{n-1} y_{n-1} B$$

mit  $Q_i \in \{\forall, \exists\}$ ,  $i < n$ , eine

- ▷ **Pränex-Normalform** oder kurz **PNF**; im bereinigten Fall spricht man von einer **bPNF**;
- ▷ **Skolem-Normalform** oder kurz **SNF**, falls es sich um eine bPNF ohne Existenzquantoren handelt, d.h.,  $Q_i = \forall$  für  $i < n$

Mit den [logischen Äquivalenzen](#) für quantifizierte Formeln sieht man leicht (HA):

## Satz

Jede Formel  $A \in \mathbf{FO}(S)$  besitzt eine äquivalente Formel  $B$  in bPNF.  $\square$

<sup>16</sup>Thoralf Albert Skolem (1887–1963)

## Vorüberlegung zur Skolemisierung

**Ziel:**  $\exists$  aus einer zur geschlossenen Formel  $A \in \mathbf{FO}(\mathcal{S})$  äquivalenten bPNF

$$B = Q_0 y_0 \cdot Q_1 y_1 \cdot \dots \cdot Q_{n-1} y_{n-1} \cdot C \quad \text{mit } C \text{ quantorenfrei}$$

so zu entfernen (**am zweckmäßigsten**, aber nicht zwingend, **von außen nach innen**), dass die resultierende Formel „erfüllbarkeitsäquivalent“ zu  $B$  ist.

Der erste Existenzquantor möge in Position  $k$  von links auftreten:

$$B = \forall y_0 \dots \forall y_{k-1} \cdot \exists y_k \cdot F \quad \text{mit } F = Q_{k+1} y_{k+1} \dots Q_{n-1} y_{n-1} \cdot C$$

In jedem Modell  $\mathcal{M} = \langle D, I \rangle$  für  $B$  gilt nun für alle  $\mathbf{u} \in D^k$  und  $\sigma \in D^\nu$

$$\sigma\{\widehat{\mathbf{y}/\mathbf{u}}\}(\exists y_k \cdot F) = \sup\{\sigma\{\widehat{\mathbf{y}/\mathbf{u}}\}\{\widehat{y_k/d}\}(F) : d \in D\} = 1$$

Die resultierende ganze(!) Relation  $D^k \xrightarrow{R_B} D$  hängt nicht von  $\sigma$  ab, da die Suprema bzw. Infima in der Auswertung von  $F$  es nicht tun.

## Zusammenhang mit (AC)

- ▶ Dem **Skolemisierungs-Trick** (s.u.) liegt folgende Annahme zugrunde:

*Aus jeder ganzen Relation  $X \xrightarrow{R} Y$  zwischen Mengen  $X$  und  $Y$  lässt sich eine Funktion  $X \xrightarrow{f} Y$  extrahieren.*

Man beachte, dass **kein** Algorithmus dafür angegeben wird!

- ▶ Obige Annahme ist im Wesentlichen das sog. **Auswahlaxiom** (AC) der Mengenlehre, das unabhängig von den übrigen Zermelo-Fraenkel Axiomen ist (vergl. Anhang C), d.h., es gibt Modelle der übrigen Axiome, die (AC) erfüllen, und solche, die das nicht tun.
- ▶ So harmlos und einleuchtend wie (AC) aussieht, hat es doch einige verblüffende und beunruhigende Konsequenzen, wie z.B. das **Banach-Tarski Paradox**. Insofern ist es immer ratsam zu wissen, welche Beweise oder Definitionen (AC) voraussetzen.

## Skolems Trick:

Formal einen funktionalen Zusammenhang zwischen  $\mathbf{y} \in \mathcal{V}^k$ , und  $y_k$  schaffen, mittels eines frischen Funktionssymbols  $f_{/k} \notin \mathbf{Fun}$ : anstatt

$$B = \forall y_0 \dots \forall y_{k-1}. \exists y_k. F$$

betrachten wir nun in  $\mathbf{FO}((\mathbf{Fun} + \{f_{/k}\}) + \mathbf{Pred})$  die Formel

$$B' = \forall y_0 \dots \forall y_{k-1}. F\{y_k/f(y_0, \dots, y_{k-1})\}$$

- ▷ Gilt (AC), lässt sich jedes Modell  $\mathcal{M} = \langle D, I \rangle$  für  $B$  zu einem Modell  $\mathcal{M}' = \langle D, I' \rangle$  für  $B'$  erweitern, indem man aus der oben beschriebenen ganzen Relation  $D^k \xrightarrow{R_B} D$  eine Interpretation von  $f_{/k}$  extrahiert.
- ▷ Umgekehrt wird aus jedem Modell  $\mathcal{M}' = \langle D, I' \rangle$  für  $B'$  durch Entfernen von  $f^{\mathcal{M}}$  aus  $I'$  ein Modell für  $B$ , denn  $D^k \xrightarrow{f^{\mathcal{M}}} D$  ist als ganze Relation in  $D^k \xrightarrow{R_B} D$  enthalten, so dass die relevanten Suprema tatsächlich den Wert 1 annehmen.

# Anmerkungen

- ▶ Jede **FO**-Formel  $A$  hat eine minimale endliche Signatur  $\mathcal{S}_A$ , in der sie formuliert werden kann. (Mittels **Signaturhomomorphismen** ließe sich das Problem **change-of-signature** sauber beschreiben; wir wollen das hier aber nicht vertiefen.)
- ▶ **Weder Reihenfolge noch Zahl der Quantoren einer (b)PNF  $B$  von  $A \in \mathbf{FO}(\mathcal{S})$  müssen eindeutig bestimmt sein** (siehe **Rechenregeln**):
  - Anstelle von (2) liefert Bereinigen und zweimalige Anwendung von (4) eine äquivalente Formel mit zwei Quantoren  $\Rightarrow$  ungeschickt!
  - Falls in (4) die Formel  $A$  die Form  $Q'y.C$  mit  $y \notin \mathbf{FV}(B)$  hat, dann können  $Qx$  und  $Q'y$  in beliebiger Reihenfolge nach außen gezogen werden, selbst wenn es sich um verschiedene Quantoren handelt. (Tipp: erst  $\exists$  nach außen ziehen, dann  $\forall$ .)
- ▶ **Folglich braucht die Signatur für Skolemisierungen von  $A \in \mathbf{FO}(\mathcal{S})$  nicht eindeutig bestimmt zu sein.** Hat man die Wahl, sind Skolem-symbole möglichst geringer Stelligkeit vorzuziehen (daher obiger Tipp).

## Beispiel (leicht psychedelisch)

Für eine Signatur  $\mathcal{S} = \{R_{/1}, S_{/2}\}$  ohne Operatoren betrachte

$$A = \forall x. \exists y. (S(x, y) \vee R(y)) \quad \text{und} \quad B = \exists y. \forall x. (R(y) \rightarrow S(y, x))$$

Um  $A \wedge B$  zu bereinigen benennt man in  $B$  die gebundenen Variablen um.

$$\begin{aligned} A \wedge B &\equiv \forall x. \exists y. (S(x, y) \vee R(y)) \wedge \exists u. \forall v. (R(u) \rightarrow S(u, v)) \\ &\equiv \forall x. \exists y. \left( (S(x, y) \vee R(y)) \wedge \exists u. \forall v. (R(u) \rightarrow S(u, v)) \right) \\ &\equiv \forall x. \exists y. \exists u. \forall v. \left( (S(x, y) \vee R(y)) \wedge (R(u) \rightarrow S(u, v)) \right) \quad (0) \end{aligned}$$

$$\text{(wg. Symmetrie)} \quad \equiv \exists u. \forall v. \forall x. \exists y. \left( (S(x, y) \vee R(y)) \wedge (R(u) \rightarrow S(u, v)) \right) \quad (1)$$

$$\begin{aligned} &\equiv \forall x. \left( \exists y. (S(x, y) \vee R(y)) \wedge \exists u. \forall v. (R(u) \rightarrow S(u, v)) \right) \\ &\equiv \forall x. \exists u. \forall v. \exists y. \left( (S(x, y) \vee R(y)) \wedge (R(u) \rightarrow S(u, v)) \right) \quad (2) \end{aligned}$$

$$\text{(wg. Symmetrie)} \quad \equiv \exists u. \forall x. \exists y. \forall v. \left( (S(x, y) \vee R(y)) \wedge (R(u) \rightarrow S(u, v)) \right) \quad (3)$$

Die markierten Formeln (0)–(3) liegen in bPNF vor.



## Beispiel (Fortsetzung)

Elimination der Existenzquantoren durch Hinzufügen geeigneter Funktionssymbole zur **Fun**-Komponente der Signatur liefert Skolem-Formeln unterschiedlicher Länge:

$$S_0 = \forall x. \forall v. \left( (S(x, f(x)) \vee R(f(x))) \wedge (R(g(x)) \rightarrow S(g(x), v)) \right) ; f_{/1}, g_{/1}$$

$$S_1 = \forall v. \forall x. \left( (S(x, h(v, x)) \vee R(h(v, x))) \wedge (R(c) \rightarrow S(c, v)) \right) ; h_{/2}, c_0$$

$$S_2 = \forall x. \forall v. \left( (S(x, k(x, v)) \vee R(k(x, v))) \wedge (R(g(x)) \rightarrow S(g(x), v)) \right) ; k_{/2}, g_{/1}$$

$$S_3 = \forall x. \forall v. \left( (S(x, f(x)) \vee R(f(x))) \wedge (R(c) \rightarrow S(c, v)) \right) ; f_{/1}, c_{/0}$$

Dies zeigt, dass Skolemisierung je nach Vorgehensweise unterschiedliche Ergebnisse liefern kann, speziell wenn verschiedene Leute dieselbe Formel bearbeiten. A priori ist nicht klar, ob es eine Strategie gibt, die immer zum kürzesten Ergebnis führt.

Es wird sich herausstellen, dass die Formeln  $A \wedge B$  und  $S_i$ ,  $i < 3$ , alle erfüllbarkeitsäquivalent im folgenden Sinne sind.

# Erfüllbarkeitsäquivalenz in der $PL_1$

## Definition (vergl. [Folie ??](#))

Die **Erfüllbarkeitsäquivalenz**  $\equiv_e$  ist die kleinste  $\subseteq_e$  umfassende ÄR auf den **abgeschlossenen** Formeln in  $FO[S]$ , wobei  $B \subseteq_e A$  gilt, sofern folgende Bedingungen erfüllt sind:

- ▷  $Fun_A \subseteq Fun_B$  und  $Pred_A = Pred_B$  für die Minimalsignaturen;
- ▷ jedes  $\mathcal{S}_B$ -Modell für  $B$  ist eingeschränkt auf  $Fun_A$  bereits ein  $\mathcal{S}_A$ -Modell für  $A$ ;
- ▷ jedes  $\mathcal{S}_A$ -Modell für  $A$  kann zu einem  $\mathcal{S}_B$ -Modell für  $B$  erweitert werden.

Offenbar handelt es sich bei  $\equiv_e$  wieder um die transitive Hülle der reflexiven und symmetrischen Relation  $\subseteq_e \cup \supseteq_e$ , und um eine echte Obermenge der Einschränkung von  $\equiv$  auf die abgeschlossenen Formeln.

# Skolemisierung

## Algorithmus (informell)

Gegeben  $A \in \mathbf{FO}(S)$ .

- ▶ Bestimme eine zu  $A$  äquivalente bPNF  $B$ ; dabei
  - bevorzuge ▶ Regel (2) gegenüber Bereinigung und Regel (4);
  - bei Anwendung von Regel (4) auf zwei Formeln mit verschiedenen ersten Quantoren, ziehe Existenz-Quantoren vor All-Quantoren nach außen, um die Stelligkeit der später benötigten Skolem-Symbole zu minimieren.
- ▶ Eliminiere die Existenz-Quantoren der resultierenden bPNF (etwa von links nach rechts) mit Hilfe passender Skolem-Symbole, die zur Signatur hinzuzufügen sind.

## Satz (HA)

Jede bPNF-Formel  $B \in \mathbf{FO}(S)$  ist zu ihrer Skolemisierung in  $\mathbf{FO}(S + \mathbf{Sko})$  erfüllbarkeitsäquivalent. □

# Das Allgemeingültigkeitsproblem $AGP(PL)$

- Gegeben:  $A \in \mathbf{FO}(\mathcal{S})$   
Frage: ist  $A$  allgemeingültig?  
oder äquivalent: ist  $\neg A$  unerfüllbar?

Es wird sich zeigen, dass tatsächlich ein Algorithmus existiert, der in endlich vielen Schritten terminiert, wenn  $\neg A$  unerfüllbar ist, aber andernfalls nicht notwendig terminiert. In der Tat existiert kein Algorithmus, der in jedem Fall terminiert. Daher ist  $AGP(PL)$ , genau wie das Unerfüllbarkeitsproblem für Formelmengen der  $AL$ , nur **semi-entscheidbar** (TheoInf 2).

Das offensichtliche Problem bei der Suche nach einem Algorithmus ist die Vielzahl der möglichen  $\mathcal{S}$ -Strukturen  $\mathcal{M} = \langle D, I \rangle$ :

- ▷ die Mächtigkeit des Datenbereichs  $D$  ist unbeschränkt;
- ▷ wir haben keine Information über  $I$ .

# Vorarbeiten zur Herbrand<sup>17</sup> Theorie: Konstanten

**Herbrands Kernaussage:** ein kanonischer Datenbereich genügt, sofern

- ▷ die Signatur **Fun** mindestens eine Konstante enthält,
- ▷ und das Symbol  $\doteq$  in  $A$  nicht vorkommt, geschrieben  $A \in \mathbf{FO}^\neq(\mathcal{S})$ .

Beide Bedingungen lassen sich immer erzwingen (Signaturen sind variabel):

Da die Datenbereiche unserer  $\mathcal{S}$ -Strukturen nicht leer sein dürfen, können wir einer Signatur  $\mathcal{S} = \mathbf{Fun} + \mathbf{Pre}$  ohne Konstanten in **Fun** problemlos eine Konstante  $c$  hinzufügen. Offenbar gilt  $\mathbf{FO}(\mathcal{S}) \subseteq \mathbf{FO}(\mathcal{S} + \{c/0\})$

Andererseits gibt es zu jedem  $B \in \mathbf{FO}(\mathcal{S} + \{c/0\})$  eine kanonische erfüllbarkeitsäquivalente Formel in  $\mathbf{FO}(\mathcal{S})$ , nämlich

$$\exists x B\{c/x\} := \exists x B\{x/c\}^{-1} \in \mathbf{FO}(\mathcal{S}) \quad \text{mit} \quad x \notin \mathbf{FV}(B)$$

<sup>17</sup> Jacques Herbrand (1908–1931)

## Vorarbeiten zur Herbrand Theorie: Eliminierung von $\doteq$

Ebenso können wir **Pred** um ein binäres Prädikat  $\mathbb{E}$  erweitern, so dass jede Formel  $A \in \mathbf{FO}(\mathcal{S})$  erfüllbarkeitssäquivalent zu einer Formel  $B \in \mathbf{FO}^{\neq}(\mathcal{S} + \{\mathbb{E}\})$  ist.  $\mathcal{S}_A$  sei die endliche(!) Minimalsignatur für  $A$ .

- ▷ OBdA möge  $A$  in bPNF vorliegen. Ersetzt man jedes Auftreten von  $\doteq$  in  $A$  durch  $\mathbb{E}$ , entsteht eine Formel  $A'$ , unter Missbrauch der Notation  $A' := A\{\doteq/\mathbb{E}\}$ . Weiter gilt  $\mathcal{S}_{A'} = \mathbf{Fun}_A + (\mathbf{Pred}_A + \{\mathbb{E}\})$ .
- ▷ Jedes Modell  $\mathcal{M}$  für  $A$  wird zu einem Modell von  $A'$ , wenn man  $\mathbb{E}^{\mathcal{M}}$  als Gleichheit interpretiert.  $A'$ -Modelle, in denen das nicht der Fall ist, liefern keine Information über die Existenz von  $A$ -Modellen.
- ▷ Bilde nun die Konjunktion  $A^{\neq}$  von  $A'$  mit endlich vielen Formeln, die jede Interpretation von  $\mathbb{E}$  zwingend zu einer Kongruenzrelation bzgl. ganz  $\mathcal{S}_A$  machen. Für jedes  $A^{\neq}$ -Modell bilden die entsprechenden Äquivalenzklassen nun ebenfalls ein  $A^{\neq}$ -Modell. Aber dort wird  $\mathbb{E}$  als Gleichheit interpretiert, also ist es auch ein  $A$ -Modell (HA).

# Der Satz von Herbrand

OBdA möge nun **Fun** eine Konstante und  $A$  kein  $\doteq$  enthalten.

## Definition

- ▷ Die **Fun**-Algebra  $D_{\mathcal{H}} := \mathbf{Term}(\mathbf{Fun}, \emptyset)$  besteht aus **Grundtermen**.
- ▷ Jede  $\mathcal{S}$ -Struktur der Form  $\mathcal{H} = \langle D_{\mathcal{H}}, I \rangle$  heißt **Herbrand-Struktur**.
- ▷ Falls  $\models_{\mathcal{H}} A$  nennen wir  $\mathcal{H}$  ein **Herbrand-Modell** von  $A$ .

Die Interpretation von **Pred** in einer Herbrand-Struktur ist frei wählbar.

Im mathematischen Sinn ist  $D_{\mathcal{H}}$  die **freie Fun-Algebra** über  $\emptyset$ ; sie ist genau dann nicht leer, wenn mindestens eine Konstante in **Fun** existiert.

## Satz (Herbrand)

Für jede Menge  $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$  geschlossener Formeln in SNF gilt:

$\Gamma$  ist erfüllbar gdw.  $\Gamma$  hat ein Herbrand-Modell

## Beweis.

Wenn  $\Gamma$  ein Herbrand-Modell hat, ist  $\Gamma$  natürlich erfüllbar.

Ist  $\mathcal{M} = \langle D, I \rangle$  ein Modell für  $\Gamma$ , so ist  $\langle D, I_{\mathbf{Fun}} \rangle$  eine **Fun**-Algebra. Die leere Abbildung  $\emptyset \xrightarrow{z} D$  lässt sich aufgrund des **Rekursionsatzes** eindeutig zu einem **Fun**-Homomorphismus  $D_{\mathcal{H}} \xrightarrow{\tilde{z}} D$  fortsetzen.

Die  $\tilde{z}$ -Urbilder der Relationen  $R^{\mathcal{M}}$ ,  $R \in \mathbf{Pred}$ , machen  $D_{\mathcal{H}}$  zu einer  $\mathcal{S}$ -Struktur  $\mathcal{M}_{\mathcal{H}}$  und  $\tilde{z}$  zu einem **starken Pred**-Homomorphismus, d.h.,

$$R^{\mathcal{M}_{\mathcal{H}}}(u_0, \dots, u_{S(R)-1}) = R^{\mathcal{M}}(\tilde{z}(u_0), \dots, \tilde{z}(u_{S(R)-1})) \quad (*)$$

für alle  $\mathbf{u} \in D_{\mathcal{H}}^{S(R)-1}$ .

**Achtung:** Dieselbe Konstruktion angewendet auf die Gleichheit über  $D$  liefert nicht notwendig die Gleichheit über  $D_{\mathcal{H}}$ , sondern i.A. nur eine Kongruenzrelation. Aus diesem Grund durfte in  $\Gamma$  kein  $\doteq$  vorkommen.

Betrachte ein beliebiges  $A \in \Gamma$ , oBdA quantifiziert über  $\mathbf{x} = \langle x_i : i < n \rangle$  und mit quantorenfreiem Teil  $B$ .



## Beweis, Fortsetzung.

Als geschlossene Formel hat  $A \in \Gamma$  eine von Belegungen unabhängige Semantik. Für beliebiges  $\tau \in (D_{\mathcal{H}})^{\vee}$  setze  $\sigma := \tilde{z} \circ \tau \in D^{\vee}$ . Wegen  $(\star)$  gilt aufgrund des Substitutionslemmas und  $\models_{\mathcal{M}} A$  für jedes  $\mathbf{u} \in (D_{\mathcal{H}})^n$ :

$$\begin{aligned} \mathcal{M}_{\mathcal{H}}[B\{\mathbf{x}/\mathbf{u}\}](\tau) &= \mathcal{M}[B\{\mathbf{x}/\tilde{z}(\mathbf{u})\}](\sigma) \\ &= \mathcal{M}[B](\sigma\{\mathbf{x}/\mathcal{M}[\tilde{z}(\mathbf{u})](\sigma)\}) = 1 \end{aligned}$$

bzw. in weniger bombastischer Notation

$$\hat{\tau}(B\{\mathbf{x}/\mathbf{u}\}) = \hat{\sigma}(B\{\mathbf{x}/\tilde{z}(\mathbf{u})\}) = \sigma\{\widehat{\sigma}(\tilde{z}(\mathbf{u}))\}(B) = 1$$

Für das Infimum über alle  $\mathbf{u} \in (D_{\mathcal{H}})^n$  folgt daher

$$\mathcal{M}_{\mathcal{H}}[A](\tau) = \mathcal{M}[A](\tilde{z} \circ \tau) = \mathcal{M}[A] = 1 \quad \text{bzw.} \quad \hat{\tau}(A) = \widehat{(\tilde{z} \circ \tau)}(A) = 1$$

Damit ist  $\mathcal{M}_{\mathcal{H}}$  ein Herbrand-Modell für  $A$ , also auch für ganz  $\Gamma$ . □

# Satz von Löwenheim<sup>18</sup>-Skolem

## Satz (Löwenheim 1915; Skolem 1922)

*Jede erfüllbare Menge  $\Gamma$  von Formeln hat ein abzählbares Modell.*

### Beweis.

$\Gamma$  ist erfüllbar gdw. das für die Menge  $\Gamma'$  der (minimalen) existenziellen Abschlüsse gilt. Deren Skolemisierung liefert eine Menge  $\Gamma''$  erfüllbarkeits-äquivalenter Formeln, die erfüllbar ist gdw. wenn das für  $\Gamma'$  gilt.

$\mathcal{M} = \langle D, I \rangle$  sei ein Modell für  $\Gamma''$ . Da sich  $\doteq$  von  $\Gamma$  auf  $\Gamma''$  vererbt, braucht  $\mathcal{M}_{\mathcal{H}}$  (s.o.) kein Modell von  $\Gamma''$  zu sein. Aber wir können  $\mathcal{M}_{\mathcal{H}}$  nach dem  $\tilde{z}$ -Urbild der Gleichheit auf  $D$  (und somit einer Kongruenzrelation auf  $D_{\mathcal{H}}$ ) faktorisieren und erhalten so ein Modell für  $\Gamma''$  und folglich auch für  $\Gamma$ . Aus der Abzählbarkeit von  $D_{\mathcal{H}}$  folgt auch die Abzählbarkeit der Quotientenmenge. □

<sup>18</sup> Leopold Löwenheim (1878–1957)

# Nichtstandard-Modelle

Die intendierte Struktur der Signatur  $\mathcal{S}_{\text{arith}} = \{0/0, 1/0, +/2, \cdot/2; </2\}$  der Arithmetik sind die natürlichen Zahlen  $\mathbb{N}$  mit den kanonischen Operationen/Relationen. Aber ist  $\mathcal{S}_{\text{arith}}$  dafür spezifisch genug?

**Ziel:** zeigen, dass es „seltsame“  $\mathcal{S}_{\text{arith}}$ -Strukturen  $\mathcal{M}^* = \langle D^*, I^* \rangle$  gibt, die dieselben geschlossenen Formeln erfüllen wie  $\mathbb{N}$  mit der kanonischen Interpretation, aber nicht zu  $\mathbb{N}$  isomorph sind.

Solche Modelle heißen **Nichtstandard-Modelle**.

**Einsicht:** Wichtige Eigenschaften z.B. der natürlichen Zahlen lassen sich mit geschlossenen Formeln in  $\mathbf{FO}(\mathcal{S}_{\text{arith}})$  nicht erfassen.

Anwendungen:

- ▶ **Nichtstandard Analysis** (Abraham Robinson, 1960);
- ▶ Computer-Algebra;
- ▶ Verifikation hybrider Systeme (Zug- und Flugzeugcontroller)

## Satz

*Es gibt Nicht-Standard-Modelle der Arithmetik.*

## Beweis.

Setze  $A_n := \underbrace{1 + \dots + 1}_{n \text{ mal}} < x$  mit freiem  $x$  und

$$\Gamma = \{ A \in \mathbf{FO}(\mathcal{S}_{\text{arith}}) : A \text{ geschlossen, und } \models_{\mathbb{N}} A \} \cup \{ A_i : i \in \mathbb{N} \}$$

Offenbar ist jede endliche Teilmenge von  $\Gamma$  erfüllbar, nämlich im Standard-Modell  $\mathbb{N}$ : da nur endlich viele Formeln der Form  $A_i$  vorkommen, findet man immer ein  $\sigma \in \mathbb{N}^{\mathcal{V}}$ , so dass  $\sigma(x)$  hinreichend groß ist.

Jedes Modell  $\mathcal{M}^*$  von  $\Gamma$  muss hingegen

- ▷ alle geschlossenen in  $\mathbb{N}$  gültigen  $\mathcal{S}_{\text{arith}}$ -Formeln erfüllen,
- ▷ ein bzgl.  $I^*(<)$  größtes Element haben, was  $\mathcal{M}^* \not\models \mathbb{N}$  impliziert.  $\square$

Lassen sich zwei  $\mathcal{S}$ -Strukturen nicht durch geschlossene  $\mathcal{S}$ -Formeln unterscheiden, werden sie **elementar äquivalent** genannt.

# Skolems Paradox

Die übliche Mengenlehre (Anhang C) ist ein Modell für die entsprechenden Axiom-Schemata. Nach dem Satz von Löwenheim-Skolem muss es aber auch ein **abzählbares Modell  $\mathcal{M}_{LS}$  von ZFC** geben.

Gemäß Anhang B ist im Standardmodell der Mengenlehre die Potenzmenge von  $\mathbb{N}$  überabzählbar. In  $\mathcal{M}_{LS}$  spielen bestimmte Elemente  $\mathcal{N}$  und  $\mathcal{P}$  die Rolle der „Menge der natürlichen Zahlen“ bzw. von deren „Potenzmenge“. Nun sollte  $\mathcal{P}$  „überabzählbar“ sein.

Warum ist das kein Widerspruch?

Die „Überabzählbarkeit“ von  $\mathcal{P}$  in  $\mathcal{M}_{LS}$  bedeutet, dass in  $\mathcal{M}_{LS}$  keine „Abbildung“ von  $\mathcal{P}$  nach  $\mathcal{N}$  „injektiv“ ist. Dagegen ist die Abzählbarkeit von  $\mathcal{M}_{LS}$  eine Aussage im Standard-Modell der Mengenlehre und kann insofern gar nicht mit der „Überabzählbarkeit“ in  $\mathcal{M}_{LS}$  in Beziehung gesetzt werden. Ein Problem entsteht erst dann, wenn man beide Modelle unzulässig vermischt (hier: die Anführungszeichen weglässt).

# Herbrand Expansion, Vorüberlegungen

Betrachte eine geschlossene bereinigte Formel in SNF

$$A = \forall x_0 \forall x_1 \dots \forall x_{n-1}. B \in \mathbf{FO}^\neq(S) \quad , \quad B \text{ quantorenfrei}$$

Deren Auswertung in einer  $\mathcal{S}_A = \mathcal{S}_B$ -Struktur  $\mathcal{M}_{\mathcal{H}}$  mit Trägermenge  $D_{\mathcal{H}}$  ist unabhängig von Belegungen  $\sigma \in (D_{\mathcal{H}})^\forall$ . Da  $\sigma$  nicht auf den variablenfreien Termen aus  $D_{\mathcal{H}}$  wirkt, gilt aufgrund des Substitutionslemmas

$$\begin{aligned} \hat{\sigma}(A) &= \inf \{ \widehat{\sigma\{\mathbf{x}/\mathbf{t}\}}(B) : \mathbf{t} \in (D_{\mathcal{H}})^n \} = \inf \{ \sigma\{\widehat{\mathbf{x}/\check{\sigma}(\mathbf{t})}\}(B) : \mathbf{t} \in (D_{\mathcal{H}})^n \} \\ &= \inf \{ \hat{\sigma}(B\{\mathbf{x}/\mathbf{t}\}) : \mathbf{t} \in (D_{\mathcal{H}})^n \} \end{aligned} \quad (*)$$

Die Werte  $\hat{\sigma}(B\{\mathbf{x}/\mathbf{t}\})$  hängen wie in der AL von den Werten der Atome, d.h., hier den Werten der atomaren Formeln  $\mathbf{AT}_{\mathcal{H}}^\neq := \mathbf{Atm}(\mathbf{Pred}_B, \mathcal{D}_{\mathcal{H}})$  ab. Aber das ist genau die  $\mathcal{M}_{\mathcal{H}}$ -Interpretation der  $\mathbf{Pred}_B$ -Prädikate in  $D_{\mathcal{H}}$ !

# Satz von Gödel<sup>19</sup>-Herbrand-Skolem

## Definition

Die **Herbrand-Expansion** der obigen Formel  $A$  besteht aus allen (parallelen) Substitution von Grundtermen (= Grundsubstitutionen) für Variablen von  $B$

$$E(A) := \{ B\{\mathbf{x}/\mathbf{t}\} : \mathbf{t} \in (D_{\mathcal{H}})^n \} \subseteq \mathcal{F}[\mathbf{AT}_{\mathcal{H}}^{\neq}] \subseteq \mathbf{FO}^{\neq}(\mathcal{S}_B)$$

Diese sind sämtlich quantorenfrei und geschlossen und folglich auf aussagenlogische Art aus  $\dot{=}$ -freien atomaren Formeln aufgebaut.

Für  $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$  ist  $E(\Gamma)$  die Vereinigung der Mengen  $E(A)$ ,  $A \in \Gamma$ .

## Satz

Für eine Menge  $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$  geschlossener Formeln in SNF gilt

$\Gamma$  ist erfüllbar gdw.  $E(\Gamma)$  ist aussagenlogisch erfüllbar

<sup>19</sup> Kurt Gödel (1906–1978)

## Beweis.

Eine  $E(\Gamma)$  erfüllenden Belegung  $\varphi$  der atomaren Formeln in  $\mathbf{AT}_{\mathcal{H}}^{\neq}$  ist nach obiger Überlegung eine Interpretation  $I_{\varphi}$  der Prädikate in  $D_{\mathcal{H}}$ . In der Herbrand-Struktur  $\mathcal{M}_{\varphi} = \langle D_{\mathcal{H}}, I_{\varphi} \rangle$  gilt nun  $\mathcal{M}_{\varphi} \llbracket A \rrbracket = 1$ , da rechts in (\*) nur die Werte  $\hat{\varphi}(B\{\mathbf{x}/\mathbf{t}\}) = 1$  auftreten.

Umgekehrt hat  $\Gamma$  ein Herbrand-Modell  $\mathcal{M}_{\mathcal{H}}$ , dessen Interpretation der Prädikate eine Belegung  $\varphi_{\mathcal{M}_{\mathcal{H}}}$  der atomaren Formeln liefert. Aus  $\mathcal{M}_{\mathcal{H}} \llbracket A \rrbracket = 1$  folgt dann gemäß (\*) auch  $\widehat{\varphi_{\mathcal{M}_{\mathcal{H}}}}(B\{\mathbf{x}/\mathbf{t}\}) = 1$  für jedes  $\mathbf{t} \in (D_{\mathcal{H}})^n$ . Also ist  $E(\Gamma)$  erfüllbar. □

In Verbindung mit dem Kompaktheitssatz der Aussagenlogik ergibt sich

## Korollar

Eine Menge  $\Gamma \subseteq \mathbf{FO}^{\neq}(\mathcal{S})$  geschlossener Formeln in SNF ist unerfüllbar, genau dann wenn eine endliche Teilmenge von  $E(\Gamma)$  unerfüllbar ist. □



## Beispiel

Für die Signatur  $\mathcal{S} = \{c_{/0}, f_{/1}, g_{/2}\} + \{P_{/1}\}$  betrachten wir einige Elemente der Herbrand-Expansion für  $A = \forall x.(P(x) \vee \neg P(f(x)))$ , sortiert nach ihrer Länge (ohne Klammern):

Länge 7:  $P(c) \vee \neg P(f(c))$

Länge 9:  $P(f(c)) \vee \neg P(f(f(c)))$

Länge 11:  $P(f(f(c))) \vee \neg P(f(f(f(c))))$  ,  $P(g(c, c)) \vee \neg P(f(g(c, c)))$

Länge 13:  $P(f(f(f(c)))) \vee \neg P(f(f(f(f(c))))$  ,

$P(g(f(c), c)) \vee \neg P(f(g(f(c), c)))$  ,

$P(g(c, f(c))) \vee \neg P(f(g(c, f(c))))$

Hier liefern die Substitutionen Klauseln in den positiven/negativen atomaren Formeln ohne Variablen, mit dem Potential zur Resolventenbildung.

Falls der quantorenfreie Teil einer Formel mehr als eine freie Variable enthält, vervielfachen sich die Möglichkeiten zur Substitution.

# Gilmores Algorithmus (ineffizient)

## Algorithmus

**Eingabe:**  $\Gamma \subseteq \mathbf{FO}^\neq(\mathcal{S})$  bestehe aus geschlossenen Formeln in SNF, und  $A_i$ ,  $i \in \mathbb{N}$ , sei eine Aufzählung von  $E(\Gamma)$ .

**Algorithmus:** Solange  $G_n := \bigwedge_{i < n} A_i$  erfüllbar ist, bilde  $G_{n+1} = G_n \wedge A_n$ .

Folgende Aussagen sind für  $\Gamma$  äquivalent:

- ▷ Der Algorithmus terminiert;
- ▷ für ein minimales  $k > 0$  gilt  $\models \neg G_k$ ;
- ▷ für ein minimales  $k > 0$  ist  $G_k$  nicht erfüllbar;
- ▷ für ein minimales  $k > 0$  ist  $\{A_i : i < k\} \subseteq E(\Gamma)$  nicht erfüllbar;
- ▷  $E(\Gamma)$  ist nicht erfüllbar;
- ▷  $\Gamma$  ist nicht erfüllbar.

Damit ist das Allgemeingültigkeitsproblem der PL semi-entscheidbar.

# Der Kompaktheitssatz der $PL_1$

## Satz

Eine Formelmenge  $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$  ist genau dann erfüllbar, wenn sie endlich erfüllbar ist, d.h., wenn jede endliche Teilmenge  $\Gamma_0 \subseteq \Gamma$  erfüllbar ist.

## Beweis.

Die Notwendigkeit ist klar.

Für die Hinlänglichkeit betrachte erst den Fall geschlossener Formeln in SNF ohne  $\doteq$ . Hier ist  $\Gamma$  genau dann erfüllbar, wenn das für  $E(\Gamma) := \bigcup \{ E(A) : A \in \Gamma \}$  gilt, was nach dem KPS(AL) zur endlichen Erfüllbarkeit von  $E(\Gamma)$  äquivalent ist.

Ist  $\Gamma$  endlich erfüllbar, finden wir zu jeder endlichen Teilmenge  $\Delta_0 \subseteq E(\Gamma)$  eine endliche und somit erfüllbare Teilmenge  $\Gamma_0 \subseteq \Gamma$  mit  $\Delta_0 \subseteq E(\Gamma_0)$ . Damit ist  $\Delta_0$  erfüllbar, und folglich ist  $E(\Gamma)$  endlich erfüllbar, woraus nach obiger Überlegung die Erfüllbarkeit von  $\Gamma$  folgt.

## Beweis, Fortsetzung.

Nun betrachte eine beliebige Menge  $\Gamma \subseteq \mathbf{FO}(\mathcal{S})$ .

- 1 Bilde die Menge  $\Gamma'$  der existentiellen Abschlüsse der Formeln in  $\Gamma$ .
- 2 Tritt  $\doteq$  in  $\Gamma'$  auf, so ersetze es durch ein frisches Prädikat  $E_{/2}$  und erweitere  $\Gamma'$  für jedes  $A \in \Gamma'$  um Formeln, die jeweils sicherstellen, dass  $E$  in jeder Struktur als Kongruenz bzgl. der Operatoren und Prädikate in  $\mathcal{S}_A$  interpretiert werden muss (vergl. HA).
- 3 Wandle die Elemente der resultierenden Menge  $\Gamma'' \subseteq \mathbf{FO}^\neq(\mathcal{S} + \{E_{/2}\})$  SNF um. Ggf. füge eine Konstante  $c_{/0}$  zur Signatur  $\mathcal{S}$  hinzu.
- 4 Behandle die resultierende Menge  $\Gamma''' \subseteq \mathbf{FO}(\mathcal{S} + \{E_{/2}\} + \mathbf{Sko} + \{c\})$  wie oben. □

# Kapitel 12

## Algorithmen

# Tableaus in der $PL_1$

Um die Tableau-Methode in die PL übertragen, klassifiziert man in  $FO^{\neq}(S)$  quantifizierte Formeln und ihre Negationen, vergl. ▶ Folie 150:

## Definition

- ▷ „Literale“: atomare Formeln und ihre Negationen;
- ▷ doppelte Negationen – überflüssig, sofort eliminieren;
- ▷  $\alpha$ :  $A \wedge B$ ,  $\neg(A \vee B)$ ,  $\neg(A \rightarrow B)$ ;
- ▷  $\beta$ :  $A \vee B$ ,  $A \rightarrow B$ ,  $\neg(A \wedge B)$ ;
- ▷  $\gamma$ :  $\forall x A$ ,  $\neg\exists x A$ ;
- ▷  $\delta$ :  $\exists x A$ ,  $\neg\forall x A$ .

Neue Regeln mit  $t \in D_{\mathcal{H}}$  bzw. **frischer Konstante**  $c$  für den aktuellen Ast:

$$\gamma: \frac{\forall x A}{A\{x/t\}} \quad , \quad \frac{\neg\exists x A}{\neg A\{x/t\}} \quad \delta: \frac{\exists x A}{A\{x/c\}} \quad , \quad \frac{\neg\forall x A}{\neg A\{x/c\}}$$

Die „Nenner“ bezeichnen wir als  $\gamma$ - bzw.  $\delta$ -Teilchen.

Während die Tableau-Methode der AL die Teilchen einer Formelmenge iterativ bestimmte und diese so in einer Baumstruktur arrangierte, dass mögliche erfüllende Belegungen bzw. deren Nichtexistenz ablesbar wurden, berücksichtigt die  $PL_1$ -Variante zudem die Skolemisierung (via  $\delta$ -Formeln) und die Konstruktion der Herbrand-Expansion (via  $\gamma$ -Formeln).

- ▶  $\delta$ -Formeln haben Vorrang; das entspricht der Eliminierung führender Existenz-Quantoren zugunsten neuer Konstanten (**Skolemisierung**).  
Diese vergrößern sukzessive die Signatur  $\mathcal{S}$ , also auch  $D_{\mathcal{H}}$ , stehen daher anschließend für Substitutionen in  $\gamma$ -Formeln zur Verfügung!
- ▶  $\gamma$ -Formeln können **wiederholt** und **beliebig oft** zu Substitutionen herangezogen werden; dies entspricht der **Herbrand-Expansion**.
- ▶ Für explizite Verzweigungen sind nur die  $\beta$ -Teilchen zuständig.

Die Begriffsbildungen der AL (vergl. ▶ Folie 159) sind nur geringfügig anzupassen. Wie zuvor beschränken wir uns auf die Menge  $FO^{\neq \neg \neg}(\mathcal{S})$  der Formeln, die **nicht** mit einer doppelten Negation beginnen.

## Definition

Ein **Tableau** der PL ist Abbildung  $\mathbb{B}^* \xrightarrow{\tau} \mathbf{P}(\mathbf{FO}^{\neq \neg \neg}(\mathcal{S}))$ , so dass

- ▷ das Urbild  $\mathcal{B}(\tau)$  der nichtleeren Formelmengen Präfix-abgeschlossen ist und für alle  $w \in \mathbb{B}^*$  erfüllt  $w0 \in \mathcal{B}(\tau)$  gdw.  $w1 \in \mathcal{B}(\tau)$ ;
- ▷  $\Gamma \subseteq \tau(\varepsilon) \subseteq \Gamma^{<\alpha, \gamma, \delta>}$  (Sättigung bzgl.  $\alpha$ -,  $\gamma$ - und  $\delta$ -Teilchen);
- ▷ für jedes  $\varepsilon \neq w \in \mathcal{B}(\tau)$  existiert  $B \in \tau(w)$  mit  $\tau(w) \subseteq \{B\}^{<\alpha, \gamma, \delta>}$  und  $B$  ist  $\beta$ -Teilchen einer Formel aus einem echten Vorgängerknoten.

Ein **Ast**  $\Theta$  von  $\mathcal{B}(\tau)$  (**maximale lineare Präfix-geordnete Teilmenge**) heißt

- ▷ **abgeschlossen**, falls  $\bigcup \tau[\Theta]$  eine Formel und ihre Negation enthält, andernfalls heißt  $\Theta$  **offen**;
- ▷ **vollständig**, falls  $\Theta$  offen ist und  $\bigcup \tau[\Theta]$ 
  - unter  $\alpha$ - und  $\gamma$ -Teilchen abgeschlossen ist;
  - mit jeder  $\beta$ -/ $\delta$ -Formel mindestens ein  $\beta$ -/ $\delta$ -Teilchen enthält.

Ein Tableau heißt **abgeschlossen/vollständig**, falls das für jeden Ast gilt.



# Übertragung der Tableau-Sätze der AL

## Lemma

Jedes Tableau  $\tau$  kann vervollständigt werden.

## Lemma (Hintikka)

Für vollständige Tableau-Astmengen gilt: „erfüllbar“ = „offen“.

## Satz

$\Gamma$  ist unerfüllbar gdw.  $\Gamma$  hat ein abgeschlossenes Tableau.

## Satz

Für  $A \in \mathbf{FO}^{\neq \neg \neg}(S)$  und  $\Gamma \subseteq \mathbf{FO}^{\neq \neg \neg}(S)$  gilt:

- $\models A$  gdw.  $\neg A$  hat ein abgeschlossenes Tableau.
- $\Gamma \models A$  gdw.  $\Gamma \cup \{\neg A\}$  hat ein abgeschlossenes Tableau.

# Die Tableau-Methode in der Praxis

## Beispiel (vergl. Aufgabe 4, Blatt 0)

Betrachte folgende Behauptung:

Jede transitive, symmetrische, volle Relation ist reflexiv.

Um sie zu überprüfen, wählen wir eine Signatur, die nur aus einem binären Prädikat  $R/2$  besteht und formalisieren die relevanten Eigenschaften:

(0) Transitivität:  $\forall x \forall y \forall z. (R(x, y) \wedge R(y, z) \rightarrow R(x, z))$

(1) Symmetrie:  $\forall x \forall y. (R(x, y) \rightarrow R(y, x))$

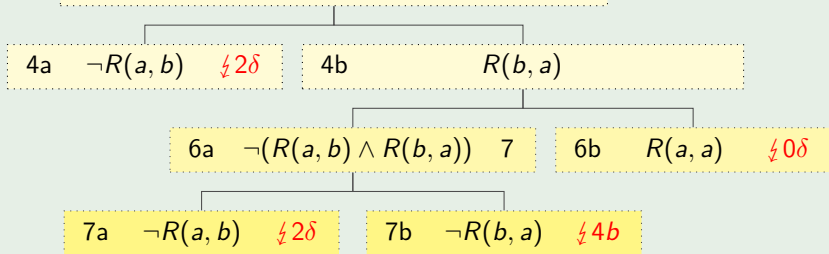
(2) Vollheit:  $\forall x \exists y. R(x, y)$

(3) Reflexivität:  $\forall x. R(x, x)$

Zum Nachweis von  $\{(0), (1), (2)\} \models (3)$  untersuchen wir mit Hilfe der Tableau-Methode, ob  $\Gamma = \{(0), (1), (2), \neg(3)\}$  **nicht** erfüllbar ist, d.h., ein abgeschlossenes Tableau hat.

## Beispiel (Fortsetzung)

*	$\forall x \forall y \forall z. (R(x, y) \wedge R(y, z) \rightarrow R(x, z))$	5
*	$\forall x \forall y. (R(x, y) \rightarrow R(y, x))$	3
*	$\forall x \exists y. R(x, y)$	1
*	$\neg \forall x. R(x, x)$	0
$0\delta$	$\neg R(a, a)$	
$1\gamma$	$\exists y. R(a, y)$	2
$2\delta$	$R(a, b)$	
$3\gamma$	$R(a, b) \rightarrow R(b, a)$	4
$5\gamma$	$R(a, b) \wedge R(b, a) \rightarrow R(a, a)$	6



# Heuristik zur Konstruktion endlicher Modelle

Im Gegensatz zur AL ist braucht die Tableau-Konstruktion für **endliche Formelmengen  $\Gamma$  nicht zu terminieren**, da die Herbrand-Expansion  $D_{\mathcal{H}}$  je nach Beschaffenheit von ***Fun*** unendlich sein kann.

Das **Gegenstück zu einer erfüllenden Belegung in der AL** wäre bei der Tableau- Methode der  $PL_1$  ein **endliches Modell**; bei abgeschlossenen Formeln spielen die Belegungen der Variablen hier keine Rolle. **Um ein solches zu finden, ändert man die Strategie, bei  $\delta$ -Formeln nur frische Konstanten für den aktuellen Ast einzuführen:**

- ▷ verwende zunächst im Ast schon vorhandene Konstanten;
- ▷ erst wenn so Widersprüche entstehen, wähle frische Konstanten.

Substituiere darüberhinaus zunächst nur Konstanten in  $\gamma$ - Formeln. Sobald die  $\gamma$ -Formeln nichts Neues liefern, bilden die bisher entlang des Zweigs eingeführten Konstanten selber den Datenbereich eines Modells für  $\Gamma$ .

## Beispiel (Endliche Modelle für $\{\exists x. \neg R(x, x), \forall x \exists y. R(x, y)\}$ )

Gibt es auf endlichen Mengen volle Relationen, die nicht reflexiv sind?

*	$\exists x. \neg R(x, x)$	0
*	$\forall x \exists y. R(x, y)$	1
$0\delta$	$\neg R(a, a)$	
$1\gamma$	$\exists y. R(a, y)$	2
$2\delta$	$R(a, b)$	
$1\gamma$	$\exists y. R(b, y)$	3
$3\delta$	$R(b, a)$	

Dies liefert ein Modell mit  $D = \{a, b\}$  und  $R_0 = \{\langle a, b \rangle, \langle b, a \rangle\}$ . Erzeugt man mit Hilfe der  $\gamma$ -Formel eine weitere Instanz von  $\exists y. R(b, y)$ , kann man diesmal  $b$  für  $y$  substituieren, was ein weiteres Model auf  $D$  mit  $R_1 = \{\langle a, b \rangle, \langle b, a \rangle, \langle b, b \rangle\}$  liefert.

**Achtung:**  $a$  und  $b$  sind zunächst Konstanten in der gemäß Skolem erweiterten Signatur. Indem wir sie hier außerdem zur Konstruktion der Modelle verwenden, interpretieren wir die Konstanten implizit.

# Resolution in der PL

Sind alle quantorenfreien Teile  $B$  der geschlossenen Skolem-Normalformen  $A \in \Gamma$  Konjunktionen prädikatenlogischer Klauseln, gehören also zu KNF, so gilt dies auch für die Elemente der Herbrand-Expansion, und wir können die Resolutions-Methode der AL anwenden.

## Beispiel

$S = \{a/0, f/1; R/1\}$  und  $A = \forall x (R(x) \wedge \neg R(f(x)))$  liefert

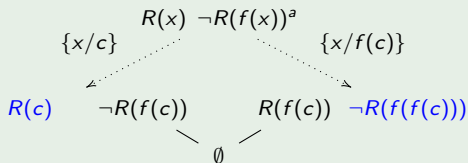
$$E(A) = \{R(a) \wedge \neg R(f(a)), R(f(a)) \wedge \neg R(f(f(a))), \dots\}$$

Die ersten beiden Elemente liefern bereits zwei Unit-Klauseln mit leerer Resolvente,  $\neg R(f(a))$  und  $R(f(a))$ . Damit ist  $A$  nicht erfüllbar.

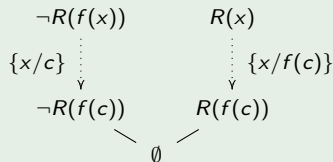
**Idee zur Vermeidung nicht-zielführender Klauseln:**  $E(A)$  „verfeinern“, indem man  $B$  als Klauselmenge auffasst und die Substitution lokal auf einzelne „vielversprechende“ Klauseln beschränkt. Das führt zur sog. **Unifikation**.

## Beispiel (Fortsetzung)

Die globalen Substitutionen  $\{x/c\}$  und  $\{x/f(c)\}$  liefern folgende Resolventenberechnung mit zwei **überflüssigen Resolventen**



Mit Hilfe lokaler Substitutionen in den  $B$ -Klauseln erhält man stattdessen



<sup>a</sup> wir lassen die Mengenklammern um die Unit-Klauseln weg, da sie mit denen der Substitutionen kollidieren.

**Problem:** die algorithmische Suche nach Grundinstanzen der  $B$ -Klauseln, die möglichst direkt zur Ableitung der leeren Klausel führen:

- ▷ systematisches Probieren der Grundsubstitutionen ist zu aufwändig;
- ▷ vorausschauende Auswahl von  $B$ -Klauseln und Grundsubstitutionen für effiziente Resolventenbildung ist sehr schwierig.

**Neue Strategie:** Suche nach beliebigen Term-Substitutionen (nicht nur Grundterme!) in  $B$ -Klauseln, die den nächsten Resolutionsschritt erlauben indem sie Literale aus verschiedenen Klauseln komplementär machen.

### Beispiel

$$\begin{array}{ccc}
 P(x), \neg Q(g(x)) & & \neg P(f(y)) \\
 & \searrow \quad \swarrow & \\
 & \{x/f(y)\} & \\
 P & & \neg Q(g(f(y)))
 \end{array}$$

Achtung: auf beiden Seiten muss dieselbe Substitution wirken!



# Unifikation

## Definition

Betrachte eine endliche Literal-Menge  $\mathcal{L}$  der  $PL_1$  (positive oder negative atomaren Formeln) **in demselben Prädikat** und eine Belegung  $\vartheta$ , die nur an endlich vielen Stellen von der Inklusion  $\mathcal{V} \xrightarrow{\iota} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$  abweicht.

- ▷ Die Substitution  $\hat{\vartheta}$  heißt **Unifikator** von  $\mathcal{L}$ , wenn alle  $\hat{\vartheta}$ -Bilder der Elemente von  $\mathcal{L}$  übereinstimmen;
- ▷  $\hat{\vartheta}$  heißt **allgemeinster Unifikator** von  $\mathcal{L}$ , wenn jeder Unifikator  $\hat{\rho}$  für  $\mathcal{L}$  durch  $\hat{\vartheta}$  faktorisiert, d.h.,  $\hat{\rho} = \hat{\vartheta}; \hat{\omega}$  für eine Substitution  $\hat{\omega}$  gilt.
- ▷  $\mathcal{L}$  heißt **unifizierbar**, wenn ein Unifikator für  $\mathcal{L}$  existiert.

## Satz (John Alan Robinson)

*Jede unifizierbare Literal-Menge hat einen allgemeinsten Unifikator.*

Existiert ein solcher für  $\mathcal{L}$ , kann er algorithmisch bestimmt werden.

# Der Unifikationsalgorithmus

## Algorithmus

**Eingabe:**  $\mathcal{L} = \{L_i : i < n\}$

**Initialisierung:**  $\vartheta := \iota$ , d.h.,  $\hat{\vartheta} = id$

- ▶ Solange  $\mathcal{L}$  von  $\hat{\vartheta}$  nicht unifiziert wird, durchsuche parallel alle  $L_i$  von links nach rechts und bestimme die erste Position, in der Unterschiede auftreten; wähle zwei dieser Literale aus.
- ▶ Falls keins dieser Literale an besagter Position eine Variable enthält, ist  $\mathcal{L}$  nicht unifizierbar.
- ▶ Andernfalls steht in einem der gewählten Literale in besagter Position die Variable  $x$ , während im anderen Literal ein Term  $t$  beginnt.
- ▶ Falls  $x \in \mathbf{FV}(t)$ , ist  $\mathcal{L}$  nicht unifizierbar.
- ▶ Andernfalls aktualisiere  $\vartheta$  zu  $\vartheta\{x/t\}$

## Beispiel

Klausel	Klausel	Klausel	Modifikation
$Q(f(a, x), u)$	$Q(f(y, g(u)), h(w))$	$Q(v, h(b))$	$\{v/f(a, x)\}$
$Q(f(a, x), u)$	$Q(f(y, g(u)), h(w))$	$Q(f(a, x), h(b))$	$\{y/a\}$
$Q(f(a, x), u)$	$Q(f(a, g(u)), h(w))$	$Q(f(a, x), h(b))$	$\{x/g(u)\}$
$Q(f(a, g(u)), u)$	$Q(f(a, g(u)), h(w))$	$Q(f(a, g(u)), h(b))$	$\{u/h(w)\}$
$Q(f(a, g(h(w))), h(w))$	$Q(f(a, g(h(w))), h(w))$	$Q(f(a, g(h(w))), h(b))$	$\{w/b\}$
$Q(f(a, g(h(b))), h(b))$	$Q(f(a, g(h(b))), h(b))$	$Q(f(a, g(h(b))), h(b))$	

Der **most general unifier (MGU)** ist somit die von der Belegung

$$\vartheta = \iota\{v/f(a, x)\}\{y/a\}\{x/g(u)\}\{u/h(w)\}\{w/b\}$$

induzierte Substitution, wobei  $\mathcal{V} \xrightarrow{\iota} \mathbf{Term}(\mathbf{Fun}, \mathcal{V})$  die Inklusion ist.

## Beispiel

Klausel	Klausel	Modifikation
$P(x, f(y))$	$P(f(a), y)$	$\{x/f(a)\}$
$P(f(a), f(y))$	$P(f(a), y)$	<del><math>\{y/f(y)\}</math></del>

# Verallgemeinerte prädikatenlogische Resolvente

## Definition

Betrachte  $PL_1$ -Klauseln  $K$  und  $K'$  mit **disjunkten Variablenmengen** (ggf. durch Umbenennen erzwingen). Falls Literale  $L_i \in K$ ,  $i < m$ , und  $L'_j \in K'$ ,  $j < n$ , existieren, so dass

$$\{\neg L_i : i < m\} \cup \{L'_j : j < n\}$$

unifizierbar ist mit allgemeinstem Unifikator  $\hat{\vartheta}$ , dann heißt

$$R := ((K - \{L_i : i < m\}) \cup (K' - \{L'_j : j < n\}))\hat{\vartheta}$$

**prädikatenlogische Resolvente** von  $K$  und  $K'$ .

Die Resolutionsregel der AL ergibt sich für  $m = n = 1$  und  $\vartheta = \iota$ , also  $\hat{\vartheta} = \mathbf{id}$ . Ob man die Literale  $L_i$  oder die Literale  $L'_j$  negiert, ist unerheblich.

## Beispiel

$$\begin{array}{ccc}
 P(f(x)), \neg Q(z), P(z) & & \neg P(y), R(g(y, a)) \\
 & \searrow \quad \swarrow & \\
 & \{z/f(x)\}\{y/f(x)\} & \\
 P & \neg Q(f(x)), R(g(f(x)), a) & 
 \end{array}$$

Hier gilt  $m = 2$  und  $n = 1$ .

- ▶ Die Handrechnung lässt sich ähnlich gestalten wie in der AL.
- ▶ Da zu resolvierende Literale dasselbe Prädikat aufweisen müssen, kann man eine Liste der zu bearbeitenden Prädikate vorgeben.
- ▶ Sind nicht alle Literale einer Klausel mit demselben Prädikat unifizierbar, muss dieses Prädikat mehrfach in der obigen Liste auftreten.
- ▶ **Dürfen Klauseln von der weiteren Betrachtung ausgeschlossen werden, wenn sie nach einer echten Unifikation tautologisch geworden sind?**
- ▶ **Wie ist mit Klauseln zu verfahren, die nach einer echten Unifikation von der resultierenden Resolvente subsumiert werden?**

## Beispiel

Weisen Sie die Allgemeingültigkeit nach:

$$A = \forall y. Q(y) \vee \neg \forall x. \left[ (Q(x) \vee R(x)) \wedge \exists z. (\neg P(z) \wedge (P(z) \vee \neg R(x))) \right]$$

Die Behauptung ist äquivalent zur Unerfüllbarkeit von  $\neg A$ . Negation und Anwendung der De Morgan'schen Regel liefert:

$$\exists y. \neg Q(y) \wedge \forall x. \left[ (Q(x) \vee R(x)) \wedge \exists z. (\neg P(z) \wedge (P(z) \vee \neg R(x))) \right]$$

Daraus ergibt sich die PNF:

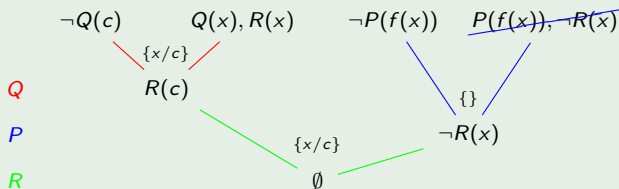
$$\exists y \forall x \exists z. [\neg Q(y) \wedge (Q(x) \vee R(x)) \wedge \neg P(z) \wedge (P(z) \vee \neg R(x))]$$

Skolemisierung liefert schließlich:

$$\forall x [\neg Q(c) \wedge (Q(x) \vee R(x)) \wedge \neg P(f(x)) \wedge (P(f(x)) \vee \neg R(x))]$$

Der quantorenfreie Teil liegt nun in KNF vor, was Resolution ermöglicht.

## Beispiel (Fortsetzung)



Damit ist die ursprünglichen Formel  $A$  nicht erfüllbar.

## Beispiel

Weisen Sie die Unerfüllbarkeit nach von

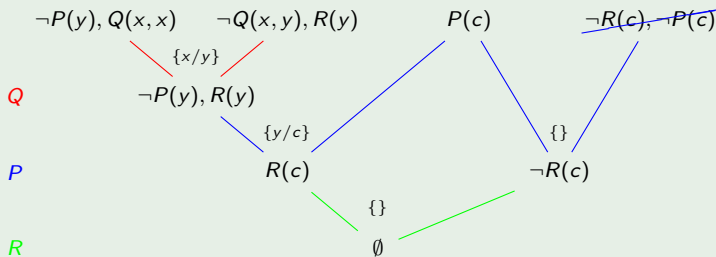
$$\exists z \forall x \forall y. [(P(y) \rightarrow Q(x, x)) \wedge (Q(x, y) \rightarrow R(y)) \wedge P(z) \wedge (\neg R(z) \vee \neg P(z))]$$

Wir beginnen mit der Skolemisierung:

$$\forall x \forall y. [(P(y) \rightarrow Q(x, x)) \wedge (Q(x, y) \rightarrow R(y)) \wedge P(c) \wedge (\neg R(c) \vee \neg P(c))]$$

Elimination von  $\rightarrow$  liefert einen quantorenfreien Teil in KNF, für Resolution:

## Beispiel (Fortsetzung)



Damit ist die ursprünglichen Formel  $A$  nicht erfüllbar.

Im ersten Schritt wäre auch die Substitution  $\{y/x\}$  möglich aber weniger effizient gewesen, da  $y$  häufiger auftritt als  $x$ .

Versuchen Sie zur Übung, andere Reihenfolgen der Prädikate zu wählen!



### Satz (Widerlegungsvollständig- und Korrektheit, John Alan Robinson)

*$A = \forall x_0 \dots \forall x_{n-1}. B$  in SNF mit  $B$  quantorenfrei in KNF ist genau dann unerfüllbar, wenn  $B \vdash_{\text{res}} \emptyset$ .*

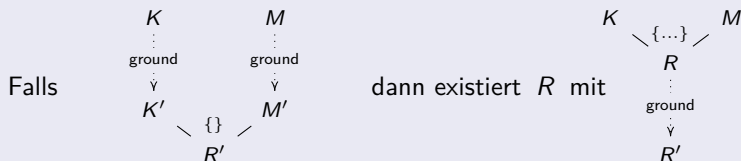
**Achtung:** Leider braucht das oben beschriebene Verfahren bei der Suche nach der Resolvente  $\emptyset$  **nicht** zu terminieren. **Daher ist das Problem der Unerfüllbarkeit hier nicht entscheidbar.**

Der Beweis zu Robinsons Satz reduziert die obige prädikatenlogische Resolventenbildung, bei der nicht-triviale Unifikationen auftreten können, auf die im Wesentlichen aussagenlogische Resolventenbildung, bei der nur Grundsubstitutionen zur Anwendung kommen.

Wesentliches Hilfsmittel ist das folgende „Lifting Lemma“:

## Lifting Lemma

Sind  $K$  und  $M$  prädikatenlogische Klauseln mit Grundinstanzen  $K'$  und  $M'$ , die eine aussagenlogische Resolvente  $R'$  haben, dann existiert eine prädikatenlogische Resolvente  $R$  von  $K$  und  $M$ , so dass  $R'$  eine Grundinstanz von  $R$  ist, in Diagrammform



Die umgekehrte Richtung ist klar: ergänze den Unifikator für die Resolventenbildung auf der rechten Seite um Modifikationen, die alle in den weg-resolvierten Literalen auftretenden Variablen auf die Konstante  $c$  abbilden. Komponiert mit der Grundsubstitution auf der rechten Seite liefert das wieder eine Grundsubstitution, die links verwendet werden kann.

# Anhänge

# Anhang A

## Signaturen und Term-Algebren

Viele mathematische Gebiete befassen sich mit Mengen, die eine zusätzliche Struktur tragen, und struktur-erhaltenden Abbildungen zwischen diesen.

Häufig beinhalten solche Strukturen auf einer Grundmenge  $X$  Operationen der Form  $X^n \xrightarrow{f} X$  der Stelligkeit  $n \in \mathbb{N}$ .

### Beispiel

- ▷ Die Addition auf den natürlichen (ganzen, rationalen, reellen...) Zahlen;
- ▷ Die Multiplikation auf den natürlichen (ganzen, rationalen, reellen...) Zahlen;
- ▷ Die Konkatenation von Wörtern in Mengen der Form  $A^*$ .
- ▷ Ausgezeichnete Elemente wie z.B. die 0 oder die 1 in den natürlichen (ganzen, rationalen, reellen...) Zahlen,  $i$  in den komplexen Zahlen, oder das leere Wort  $\varepsilon \in A^*$ .
- ▷ Unäre Operationen wie die Multiplikation mit  $-1$ , oder der Übergang von einer komplexen Zahl  $c = a + bi$  zur konjugiert komplexen Zahl  $\bar{c} = a - bi$ , oder die Spiegelung eines Worts aus  $A^*$ .

# Signaturen und deren Algebren

Bestehen die relevanten Strukturen ausschließlich aus Operationen, die ggf. noch gewissen **Gleichungen** (s.u.) genügen müssen, spricht man gemeinhin von **algebraischen Strukturen**.

Zwecks Abstraktion unterscheidet man in der sog. **universellen Algebra** Strukturen zunächst gemäß ihres **Typs**, d.h., wieviele Operationen welcher Stelligkeit auftreten. Dieser lässt sich in Form einer Abbildung  $\mathbf{Fun} \xrightarrow{\mathcal{S}} \mathbb{N}$  beschreiben, genannt **Signatur**. Die Elemente von  $\mathbf{Fun}$  heißen **Operatoren**. Für konkrete Anwendungen sind diese zu **interpretieren**:

## Definition

Eine **Algebra**  $\langle X, I \rangle$  des Typs  $(\mathbf{Fun} \xrightarrow{\mathcal{S}} \mathbb{N})$ , kurz  **$\mathcal{S}$ -Algebra**, besteht aus

- ▷ einer Menge  $X$ ;
- ▷ einer Operation  $X^{\mathcal{S}(g)} \xrightarrow{I(g)} X$  für jeden Operator  $g \in \mathbf{Fun}$ .

# Homomorphismen sind genauso wichtig wie Algebren

## Definition

Sind  $\langle X, I \rangle$  und  $\langle Y, J \rangle$  Algebren des Typs  $(\mathbf{Fun} \xrightarrow{\mathcal{S}} \mathbb{N})$ , so heißt eine Abbildung  $X \xrightarrow{f} Y$  **Homomorphismus**, sofern für jedes  $g \in \mathbf{Fun}$  gilt

$$\begin{array}{ccc}
 X^{\mathcal{S}(g)} & \xrightarrow{f^{\mathcal{S}(g)}} & Y^{\mathcal{S}(g)} \\
 I(g) \downarrow & & \downarrow J(g) \\
 X & \xrightarrow{f} & Y
 \end{array}$$

wobei  $f^{\mathcal{S}(g)}$  komponentenweise wie  $f$  operiert. Explizit heißt das

$$f(I(g)(\mathbf{x})) = J(g)\langle f(x_i) : i < \mathcal{S}(g) \rangle$$

für alle  $\mathbf{x} = \langle x_i : i < \mathcal{S}(g) \rangle \in X^{\mathcal{S}(g)}$ .

# Termalgebren

## Definition

Für eine Signatur  $\mathbf{Fun} \xrightarrow{\mathcal{S}} \mathbb{N}$  und eine Menge  $\mathcal{V}$  ist  $\mathbf{Term}(\mathcal{S}, \mathcal{V})$ , die Menge der **syntaktischen  $\mathcal{S}$ -Terme über  $\mathcal{V}$** , die kleinste Teilmenge von  $(\mathbf{Fun} + \mathcal{V})^*$  mit folgenden Abschlusseigenschaften:

- ▷  $\mathcal{V} \subseteq \mathbf{Term}(\mathcal{S}, \mathcal{V})$ ;
- ▷ für jedes  $g \in \mathbf{Fun}$  und  $\mathbf{t} = \langle t_i : i < \mathbf{arg} \, g \rangle \in \mathbf{Term}(\mathcal{S}, \mathcal{V})^{\mathcal{S}(g)}$  gilt

$$g\mathbf{t} = g t_0 \dots t_{\mathcal{S}(g)-1} \in \mathbf{Term}(\mathcal{S}, \mathcal{V})$$

In  $\mathbf{Term}(\mathcal{S}, \mathcal{V})$  haben die Operatoren aus  $\mathcal{S}$  eine kanonische Interpretation

$$\Phi(g)\mathbf{t} := g\mathbf{t}$$

$\langle \mathbf{Term}(\mathcal{S}, \mathcal{V}), \Phi \rangle$  heißt **freie  $\mathcal{S}$ -Algebra über  $\mathcal{V}$** .

Vereinfachend schreiben wir meist  $g$  statt  $\Phi(g)$ .



# Strukturelle Induktion

Obige induktiven Definition von **Term**( $S, \mathcal{V}$ ) impliziert ein Beweisprinzip:

## Satz

*E sei eine Eigenschaft, die  $S$ -Terme haben können oder nicht. Sofern*

- ▷ *jedes  $v \in \mathcal{V}$  Eigenschaft E hat, und*
- ▷ *für jedes  $g \in \mathbf{Fun}$  folgt aus der Eigenschaft E für alle Komponenten von  $t \in \mathbf{Term}(S, \mathcal{V})^{S(g)}$  die Eigenschaft E für  $gt$ ,*

*haben alle  $S$ -Term über  $\mathcal{V}$  Eigenschaft E.*



## Folgerung. (HA)

Jeder  $S$ -Term über  $\mathcal{V}$  kann auf genau eine Weise aus einfacheren derartigen Termen konstruiert werden. Insbesondere ist kein echtes Präfix und kein echtes Postfix eines  $S$ -Terms über  $\mathcal{V}$  ein derartiger Term.

# Klammern oder keine Klammern, das ist hier die Frage

Obige sog. ▶ polnische Notation  $gt$  für einen mit Hilfe von  $g \in \mathbf{Fun}$  konstruierten Term enthält **keine Klammern** (und somit keine Redundanz), denn die Elemente der disjunkten (!) Vereinigung  $\mathbf{Fun} + \mathcal{V}$  sind eindeutig unterscheidbar, auch wenn sie zu Wörtern konkateniert wurden.

- ▶ Zwecks **besserer Lesbarkeit** von Termen erlauben wir aber, statt  $gt$  auch  $g(\mathbf{t})$  oder  $g(t_0, \dots, t_{\mathcal{S}(g)-1})$  zu schreiben. Klammern und Kommata sind aber **nicht Teil des Terms**. Sie helfen dabei, die  $\mathcal{S}(g)$  rechts auf  $g$  folgenden Terme  $t_i$  schneller zu identifizieren.
- ▶ Bei der sog. ▶ umgekehrt polnische Notation  $tg = t_0 \dots t_{\mathcal{S}(g)-1} g$  für Terme sind beim Lesen von  $g$  (von links nach rechts) alle  $\mathcal{S}(g)$  relevanten Terme  $t_i$  bereits bekannt, sie liegen z.B. auf einen **Stack** (vergl. frühere HP Taschenrechner), dessen erste  $\mathcal{S}(g)$  Level beim Auswerten von  $g$  verschwinden (ENTER-Taste!). Andere Beispiele: PostScript, Forth.
- ▶ Die **Infix-Schreibweise** für binäre Operatoren in  $\mathcal{S}$ , etwa in der AL, **braucht zwingend Klammern**: z.B. ist  $A \rightarrow B \rightarrow C$  uneindeutig!

# Der Rekursionsatz

Diverse Konstruktionen in der AL wie auch der  $PL_1$  basieren auf der Anwendung des folgenden Rekursionsatzes. Statt dort das Rad immer wieder neu zu erfinden, formulieren wir ihn hier in allgemeiner Form:

## Satz

Ist  $\langle X, I \rangle$  eine Algebra des Typs  $\mathbf{Fun} \xrightarrow{\mathcal{S}} \mathbb{N}$ , dann lässt sich jede **Belegung der Variablen**  $\mathcal{V} \xrightarrow{\varphi} X$  **eindeutig** zu einem  $\mathcal{S}$ -Homomorphismus  $\langle \mathbf{Term}(\mathcal{S}, \mathcal{V}), \Phi \rangle \xrightarrow{\bar{\varphi}} \langle X, I \rangle$  fortsetzen.

## Beweis.

**Existenz:** Definiere  $\bar{\varphi}$  induktiv:

- ▷  $\bar{\varphi}(v) := \varphi(v)$  für  $v \in \mathcal{V}$ ;
- ▷  $\bar{\varphi}(g(\mathbf{t})) := I(g)\langle \bar{\varphi}(t_0), \dots, \bar{\varphi}(t_{\mathcal{S}(g)-1}) \rangle$  für  $g \in \mathcal{S}$  und  $\mathbf{t} = \langle t_i : i < \mathcal{S}(g) \rangle \in \mathbf{Term}(\mathcal{S}, \mathcal{V})^{\mathcal{S}(g)}$ .

Nach Konstruktion ist dies ein  $\mathcal{S}$ -Homomorphismus, der  $\varphi$  fortsetzt.

## Fortsetzung.

**Eindeutigkeit:** Ist  $\langle \mathbf{Term}(\mathcal{S}, \mathcal{V}), \Phi \rangle \xrightarrow{\psi} \langle X, I \rangle$  ein  $\mathcal{S}$ -Homomorphismus, der  $\varphi$  fortsetzt, so wenden wir strukturelle Induktion an:

**Anfang:** für jedes  $v \in \mathcal{V}$  gilt

$$\bar{\varphi}(v) = \varphi(v) = \psi(v)$$

**Annahme:** Für  $g \in S$  und  $\mathbf{t} = \langle t_i : i < S(g) \rangle \in \mathbf{Term}(\mathcal{S}, \mathcal{V})^{S(g)}$  gelte

$$\bar{\varphi}(t_i) = \psi(t_i) \quad , \quad i < S(g)$$

**Schluss:**

$$\begin{aligned} \bar{\varphi}(g(\mathbf{t})) &= I(g)\langle \bar{\varphi}(t_0), \dots, \bar{\varphi}(t_{S(g)-1}) \rangle \\ &= I(g)\langle \psi(t_0), \dots, \psi(t_{S(g)-1}) \rangle = \psi(g(t_0, \dots, t_{S(g)-1})) \end{aligned}$$

Somit stimmt  $\bar{\varphi}$  auf  $g$ -Termen mit  $\psi$  überein, also überall. [▶ back](#)



# Anhang B

## Abzählbarkeit

# Abzählbarkeit

$\mathbb{N}$  bezeichnet die unendliche Menge  $\{0, 1, 2, \dots\}$  der natürlichen Zahlen.

## Definition

Eine Menge  $B$  heißt **abzählbar**, wenn es eine injektive Abbildung  $B \xrightarrow{f} \mathbb{N}$  gibt. Andernfalls heißt sie **überabzählbar**.

Insbesondere ist jede endliche Menge abzählbar. Um diese auszuschließen, spricht man von **abzählbar unendlichen Mengen**.

## Satz.

Folgende Bedingungen für  $B$  sind äquivalent:

- (a)  $B$  ist abzählbar.
- (b)  $B = \emptyset$  oder es gibt eine surjektive Abbildung  $\mathbb{N} \xrightarrow{g} B$ .
- (c) Es gibt eine surjektive **partielle** Abbildung  $\mathbb{N} \xrightarrow{h} B$ . □

Solch ein  $g$  oder  $h$  heißt dann **Aufzählung** von  $B$ .

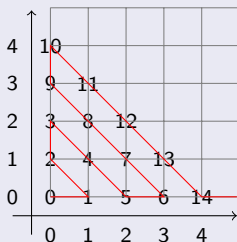
## Satz

*Teilmengen, endliche cartesische Produkte und abzählbare Vereinigungen abzählbarer Mengen sind wieder abzählbar. Dagegen sind Potenzmengen abzählbar unendlicher Mengen überabzählbar.*

## Beweis.

**Teilmengen:** Komponiere die injektive Inklusion  $C \xrightarrow{\iota} B$  mit  $B \xrightarrow{f} \mathbb{N}$ .

**Cartesisches Produkt:** Es genügt,  $\mathbb{N} \times \mathbb{N}$  als abzählbar nachzuweisen. Eine Injektion ist z.B. gegeben durch



## Beweis (Fortsetzung).

**Abzählbare Vereinigungen:** Es genügt, die disjunkte Vereinigung von  $\mathbb{N}$  Kopien von  $\mathbb{N}$  als abzählbar nachzuweisen (warum?). Aber eine derartige Vereinigung ist isomorph zu  $\mathbb{N} \times \mathbb{N}$ .

**Unendliche Potenzmengen:** Es genügt zu zeigen, dass  $\mathcal{P}(\mathbb{N})$  überabzählbar ist. Wir verfahren indirekt: ist  $\mathcal{P}(\mathbb{N}) \xrightarrow{g} \mathbb{N}$  injektiv, so betrachten wir die Menge

$$K := \{g(B) : B \subseteq \mathbb{N} \wedge g(B) \notin B\} \subseteq \mathbb{N}$$

Wegen der Injektivität von  $g$  ist  $K$  das einzige  $g$ -Urbild von  $g(K)$ . Gilt  $g(K) \in K$ , muss das aufgrund von  $g(K) \notin K$  der Fall sein. Umgekehrt kann  $g(K) \notin K$  nur aufgrund von  $g(K) \in K$  gelten, Widerspruch. (Dieses Argument funktioniert für jede unendliche Menge  $X$  und zeigt, dass keine injektive Abbildung von  $\mathcal{P}(X)$  nach  $X$  existiert.)  $\square$



## Lemma

Ist  $X$  abzählbar, so auch die Menge aller endlichen Wörter (= Tupel) über  $X$ , d.h., die disjunkte Vereinigung

$$X^* := \sum_{i \in \mathbb{N}} X^i = X^0 + X^1 + X^2 + \dots$$

## Beweis.

Es handelt sich um eine disjunkte Vereinigung endlicher cartesischer Produkte abzählbarer Mengen, und diese ist nach obigem Satz abzählbar.  $\square$

## Korollar.

Die Menge  $\mathcal{F}[\mathcal{A}]$  aller aussagenlogischen Formeln ist abzählbar.

## Beweis.

Es handelt sich um eine Teilmenge von  $(\mathcal{A} + \mathcal{J})^*$ .  $\square$

## Lemma

Für jede abzählbare Signatur  $\mathcal{S}$  ist die Menge  $\mathbf{FO}(\mathcal{S})$  aller prädikatenlogischen Formeln abzählbar.

## Beweis.

Da  $\mathcal{V}$  abzählbar ist, gilt das auch für  $(\mathcal{S} + \mathcal{V})^*$  und somit für die Teilmenge  $\mathbf{Term}(\mathbf{Fun}, \mathcal{V})$ . Die atomaren Formeln sind nun Wörter über den Alphabet  $\mathbf{Term}(\mathbf{Fun}, \mathcal{V}) + \mathbf{Pred} + \{(\, , )\}$ , bilden also auch eine abzählbare Menge. Nun greift im Wesentlichen dasselbe Argument, wie für die Aussagenlogik: mittels abzählbar vieler Junktoren lassen sich nur abzählbar viele endliche Formeln erzeugen. □

# Anhang C

## Zermelo-Fraenkel Mengenlehre und AC

## ZFC

Die übliche Zermelo<sup>20</sup>-Fraenkel<sup>21</sup> Mengenlehre lässt sich z.B. mit der Signatur  $\mathcal{S}_{\text{set}} = \{\emptyset/0; \in/2\}$  formulieren und basiert auf 8 Axiom-Schemata:

- ▷ **Extensionalität:** zwei Mengen stimmen genau dann überein, wenn sie dieselben Elemente haben:

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x \doteq y)$$

- ▷ **Leere Menge:** die Menge  $\emptyset$  hat keine Elemente:

$$\forall x \neg(x \in \emptyset)$$

- ▷ **Paarmengen:** Aus je zwei Mengen lässt sich eine neue Menge mit genau diesen Elementen bilden (ungeordnete Paare):

$$\forall x \forall y \exists z \forall w (w \in z \leftrightarrow (w \doteq x \vee w \doteq y))$$

Schreibweise:  $\{x, y\}$  für  $z$ .

<sup>20</sup> Ernst Friedrich Ferdinand Zermelo (1871–1953)

<sup>21</sup> Abraham Halevi Fraenkel (1891–1965)

- ▷ **Vereinigung**: je zwei Mengen können vereinigt werden:

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists w (z \in w \wedge w \in x))$$

Schreibweise:  $\bigcup x$  für  $y$ , oder  $u \cup v$  falls  $x = \{u, v\}$ .

- ▷ **Unendlichkeit**: es gib eine unendliche Menge:

$$\exists x (\emptyset \in x \wedge \forall y (y \in x \rightarrow y \cup \{y\} \in x))$$

- ▷ **Potenzmengen**: zu jeder Menge kann man die Menge ihrer „Teilmengen“ bilden:

$$\forall x \exists y \forall z (z \in y \leftrightarrow \forall w (w \in z \rightarrow w \in x))$$

Schreibweise:  $\mathbf{P}(x)$  für  $y$ .

- ▷ **Regularität** oder **Fundierung**: jede nichtleere Menge enthält ein zu ihr disjunktes Element:

$$\forall x \left( \neg(x \doteq \emptyset) \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)) \right)$$

- ▷ **Aussonderung**: zu jedem in ZF ausdrückbaren Eigenschaft existiert zu jeder Menge die Teilmenge derjenigen Elemente mit dieser Eigenschaft:  
 Falls  $\mathbf{FV}(A) \subseteq \{x, z\} \cup \{w_i : i < n\}$  (Metasprache!), dann

$$\forall x \forall w_0 \cdots \forall w_{n-1} \exists y \forall z (z \in y \leftrightarrow z \in x \wedge A)$$

Schreibweise:  $\{z : z \in x \wedge A\}$  oder  $\{z \in x : A\}$  für  $y$ .

- ▷ **Auswahl** (Choice), wird von Praktikern oft hinzugenommen: aus jedem Element  $u$  einer Menge  $x$  paarweise disjunkter nichtleerer Mengen kann man jeweils genau ein ( $\exists!$ ) Element auswählen:

$$\forall x \left( (\emptyset \notin x) \wedge \forall y \forall z (y \in x \wedge z \in x \rightarrow x \dot{\neq} y \vee \neg \exists w (w \in x \wedge w \in y)) \right. \\ \left. \rightarrow \exists w \forall u (u \in x \rightarrow \exists! v (v \in u \wedge v \in w)) \right)$$

Ein großer Teil der üblichen Mathematik lässt sich in ZFC formulieren, etwa die Konzepte einer natürlichen Zahl, der Menge  $\mathbb{N}$ , einer Funktion, der Injektivität, der Surjektivität, der Abzählbarkeit, etc.