

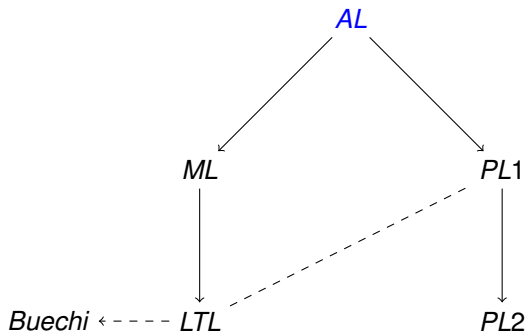
# Formale Systeme - Schnelldurchlauf

## Tutorium 42

Sebastian Buchwald

Universität Karlsruhe

5. Februar 2008



# Motivation

Anwendungen:

- 70-Damenproblem
- Sudoku

Man stößt aber doch recht schnell an die Grenzen der Aussagenlogik.

# Syntax der Aussagenlogik

- $\Sigma$  abzählbare Menge der Atome



# Formeln der Aussagenlogik

- $1 \in For_{0\Sigma}$
- $0 \in For_{0\Sigma}$
- $\Sigma \subseteq For_{0\Sigma}$

Sind  $A$  und  $B$  Formeln, dann auch

- $\neg A$
- $(A \wedge B)$
- $(A \vee B)$
- $(A \rightarrow B)$
- $(A \leftrightarrow B)$



# Semantik der Aussagenlogik

Eine **Interpretation** ist eine Abbildung

$$I : \Sigma \rightarrow \{W, F\}.$$

Eine Auswertung ist die eineindeutige Fortsetzung einer Interpretation auf Formeln

$$val_I : For_0\Sigma \rightarrow \{W, F\}$$

mit

- $val_I(0) = F$
- $val_I(1) = W$
- ...



# Modell

Eine Interpretation  $I$  heißt **Modell** einer Formel  $A$  wenn

$$val_I(A) = W.$$

Eine Formel heißt **erfüllbar** wenn sie ein Modell besitzt.

Eine Formel heißt **allgemeingültig** wenn jede Interpretation ein Modell ist.

Allgemeingültige Formeln der **Aussagenlogik** heißen auch **Tautologien**.



# Logische Folgerbarkeit

Sei  $M$  eine Formelmenge und  $A, B$  Formeln. Es gilt

$$M \models A$$

wenn jedes Modell von  $M$  (d.h. jedes Modell aller  $C \in M$ ) auch Modell von  $A$  ist.

Wir schreiben

$$A \equiv B$$

wenn gilt  $A \models B$  und  $B \models A$ .

Was bedeutet  $\models A$  ?



# Logische Folgerbarkeit

Sei  $M$  eine Formelmenge und  $A, B$  Formeln. Es gilt

$$M \models A$$

wenn jedes Modell von  $M$  (d.h. jedes Modell aller  $C \in M$ ) auch Modell von  $A$  ist.

Wir schreiben

$$A \equiv B$$

wenn gilt  $A \models B$  und  $B \models A$ .

Was bedeutet  $\models A$  ?



## Typische Fragen

Sei  $A$  eine Formel.

- Ist  $A$  erfüllbar?
  - NP-vollständig.
  - Für Hornformel in quadratischer Zeit entscheidbar.
- Ist  $A$  allgemeingültig?
  - Für Äquivalenzformeln in linearer Zeit entscheidbar.



# Kalküle

Mit Kalkülen lassen sich Aussagen **rein syntaktisch** beweisen.

Sei  $M$  eine Formelmenge und  $A$  eine Formel.

Ein Kalkül heißt **korrekt** wenn gilt

$$M \vdash A \Rightarrow M \models A.$$

Ein Kalkül heißt **vollständig** wenn gilt

$$M \models A \Rightarrow M \vdash A.$$



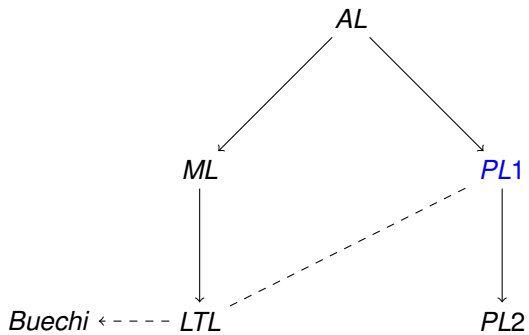
# Kalküle für Aussagenlogik

- Hilbert-Kalkül
- Resolutionskalkül
  - Widerlegungskalkül
  - Voraussetzung: KNF
- Tableauekalkül
  - Widerlegungskalkül
  - Liefert Gegenbeispiel (wenn  $M$  endlich)
- Sequenzenkalkül

Kein Kalkül sondern Algorithmus:

- Davis-Putnam
  - Voraussetzung: KNF





# Motivation

Anwendungen:

- Sokrates
- Trinker-Paradoxon (Smullyan)

Im Gegensatz zu Aussagenlogik können wir nun Aussagen über Elemente eines Universums machen.

# Syntax der PL1

Eine Signatur  $\Sigma = (P_\Sigma, F_\Sigma, \alpha_\Sigma)$  besteht aus

- einer endlichen oder abzählbar unendlichen Menge  $P_\Sigma$  der Prädikatssymbole
- einer endlichen oder abzählbar unendlichen Menge  $F_\Sigma$  der Funktionssymbole
- der Stelligkeit  $\alpha_\Sigma : (P_\Sigma \cup F_\Sigma) \rightarrow \mathbb{N}$



# Terme

- Variablen sind Terme
- Ist  $f$  ein  $n$ -stelliges Funktionssymbol und  $t_1, \dots, t_n$  Terme, dann ist auch

$$f(t_1, \dots, t_n)$$

ein Term.



# Formel der PL1

## Atomare Formeln:

- $s \doteq t$  wobei  $s, t$  Terme
- $p(t_1, \dots, t_n)$  wobei  $p$   $n$ -stelliges Prädikat,  $t_1, \dots, t_n$  Terme

Sind  $A, B$  Formeln und  $x$  eine Variable. Dann sind auch

- $A \circ B$  (siehe Aussagenlogik)
- $\forall xA$
- $\exists xA$

Formeln.



# Semantik der PL1

Eine **Interpretation** ist ein Paar  $(D, I)$  wobei

- $D$  eine **nichtleere** Menge
- $I$  Abbildung der Signatursymbole wie folgt:
  - für Konstanten (0-stellige Funktionen)  $I(c) \in D$
  - für  $n$ -stellige Funktionen  $I(f) : D^n \rightarrow D$
  - für 0-stellige Prädikate  $I(P) \in \{W, F\}$
  - für  $n$ -stellige Prädikate  $I(P) \subseteq D^n$



# Variablenbelegung

Im Gegensatz zur Aussagenlogik hängt die **Auswertung** nicht nur von der Interpretation ab. Ein weiterer Faktor ist die **Variablenbelegung**

$$\beta : Var \rightarrow D.$$



# Modell

Eine Interpretation  $(D, I)$  heißt **Modell** einer Formel  $A$  wenn **für alle** Variablenbelegungen  $\beta$  gilt:

$$val_{D,I,\beta}(A) = W.$$

Was heißt nochmal  $M \models A$  ?



## Allgemeingültigkeit und Erfüllbarkeit

Eine Formel heißt **allgemeingültig** wenn jede Interpretation ein Modell ist.

Eine Formel heißt **erfüllbar** wenn es eine Interpretation  $(D, I)$  und **eine** Variablenbelegung  $\beta$  gibt mit

$$val_{D,I,\beta}(A) = W.$$

Gibt es eine erfüllbare Formel, die kein Modell hat ?



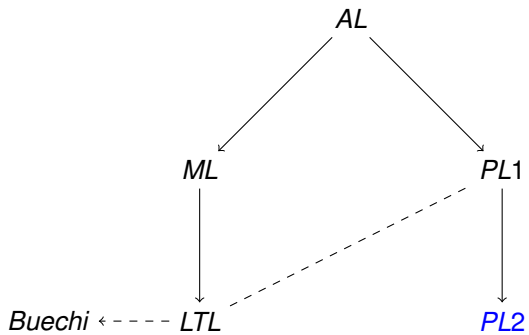
Für die Kalküle braucht man im Vergleich zur Aussagenlogik mehr Handwerkszeug:

- Normalformen:
  - Negationsnormalform
  - bereinigte Form
  - Pränex-Normalform
  - Skolem-Normalform
- Unifikatoren
- Herbrand-Strukturen



# Kalküle

- Tableaunkalkül
  - Voraussetzung: Allabschluss
  - Termersetzungssysteme für Gleichheit
- Sequenzkalkül



## Formel der PL2

### Atomare Formeln:

- $X(t)$  wobei  $X$  Mengevariable und  $t$  ein Term Terme

Ist  $A$  eine Formel dann sind auch

- $\forall X A$
- $\exists X A$

Formeln.



# Variablenbelegung

Die **Auswertung** hängt von zwei **Belegung** ab:

$$\beta : IVar \rightarrow D$$

$$\gamma : MVar \rightarrow P(D).$$



# Modell

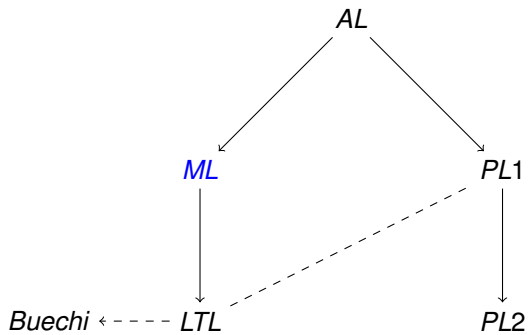
Eine Interpretation  $(D, I)$  heißt **Modell** einer Formel  $A$  wenn **für alle** Belegungen  $\beta, \gamma$  gilt:

$$val_{D, I, \beta, \gamma}(A) = W.$$



# Kalküle

Es gibt keine korrekten und vollständigen Kalküle für PL2.



# Motivation

Man hat verschiedene Welten und Übergänge zwischen den Welten.  
Der Wahrheitswert einer Aussage ist von der Welt abhängig.

Beispiel

- Drei Weisen



# Formeln der Modallogik

Ist  $A$  eine Formel, dann auch

- $\Box A$
- $\Diamond A$



# Semantik der Modallogik

Eine **Kripke-Struktur** ist ein Tupel

$$(S, R, I)$$

mit

- $S$  nichtleere Menge der **Welten**
- $R \subseteq S \times S$  Zugänglichkeitsrelation zwischen den Welten
- $I: (\Sigma \times S) \rightarrow \{W, F\}$



# Gültigkeit einer Formel

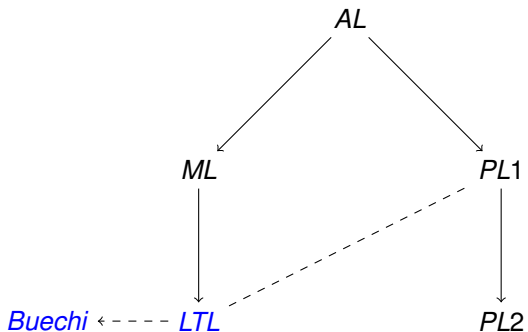
Sei  $\mathcal{K} = (S, R, I)$  eine Kripke-Struktur

$$(\mathcal{K}, s) \models A \Leftrightarrow \text{val}_s(A) = W$$

$$\mathcal{K} \models A \Leftrightarrow \text{für alle } s \in S : (\mathcal{K}, s) \models A$$

$$(S, R) \models A \Leftrightarrow \text{für alle } I : (S, R, I) \models A$$





# Motivation

**Lineare Temporale Logik** ist eine modale Logik.

Beispiel

- Telefonvermittlung



## Formeln (LTL)

Sind  $A$  und  $B$  Formeln, dann auch

- $\Box A$
- $\Diamond A$
- $A \mathcal{U} B$
- $\mathcal{X} A$



# Semantik der Modallogik

Eine **Omega-Struktur** ist ein Tupel

$$\mathcal{R} = (\mathbb{N}, <, \xi)$$

mit

- $\mathbb{N}$  natürliche Zahlen
- $<$  natürlich die natürliche Ordnung der natürlichen Zahlen
- $\xi : \mathbb{N} \rightarrow 2^\Sigma$  ( $\Sigma$  ist AL-Signatur)

$$\mathcal{R} \models p \Leftrightarrow p \in \xi(0)$$



# LTL und Büchi-Automaten

Jede Omega-Struktur kann als unendliches Wort über

$$V = 2^\Sigma$$

aufgefasst werden.

Zu jeder LTL-Formel  $B$  gibt es einen Büchi-Automaten  $A_B$  mit

$$L^\omega(A_B) = \{\xi \in V^\omega \mid \xi \models B\}.$$

