

Computational Logic

Ralf Moeller
Hamburg Univ. of Technology

Acknowledgements

- Material für diese Vorlesung wurde zu einem Teil übernommen von
 - ◆ <http://www.fmi.uni-stuttgart.de/szs/teaching/ws0809/logik/inhalt.shtml>

Historischer Überblick

- Aristoteles (384 - 322 v. Chr.): Syllogismus
 - „Jeder Grieche ist ein Mensch
 - Jeder Mensch ist sterblich
 - > Jeder Grieche ist sterblich“
- Boole (1815-1864): Aussagenlogik als Algebra
- Frege (1848-1929): Prädikatenlogik
- Russell(1872-1970): Antinomien, Typisierung
- Church (1903-1995): Lambda-Kalkül
- Gödel (1906-1978): Unentscheidbarkeit
- Gentzen (1909-1945): Sequenzenkalkül
- 1954-58: Erste maschinelle Beweise
- 1963ff: Unifikation und Resolution
- 1970ff: Prolog
- 1985ff: Beweisen in nichtklassischen Logiken

Hilbert-Kalkül (1)

Wir betrachten die folgenden fünf **Axiomenschemata** oder **Axiome**.

$$(1) F \rightarrow (G \rightarrow F)$$

$$(2) (F \rightarrow (G \rightarrow H)) \rightarrow ((F \rightarrow G) \rightarrow (F \rightarrow H))$$

$$(3) (\neg F \rightarrow \neg G) \rightarrow (G \rightarrow F)$$

$$(4) F \rightarrow (\neg F \rightarrow G)$$

$$(5) (\neg F \rightarrow F) \rightarrow F$$

Eine Formel, die nach diesem Muster gebildet wird, heißt **Instanz eines Axioms**. Jede Instanz eines Axioms ist eine gültige Formel.

Beispiel: Instanz von Axiom (4) mit $F = \neg A \rightarrow B$, $G = \neg C$

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

Hilbert Kalkül (2)

Sei M eine Menge von Formeln - auch Menge von *Hypothesen* genannt - und F eine *Formel*.

Wir schreiben $M \vdash F$ und sagen F ist im Hilbert-Kalkül aus M herleitbar, genau dann, wenn eine der folgenden Bedingungen erfüllt ist:

Axiom: F ist Instanz eines Axioms oder

Hypothese: $F \in M$ oder

Modus Ponens: es gilt $M \vdash G \rightarrow F$ und $M \vdash G$

Hilbert Kalkül (3)

Schlußregel des Kalküls:

$$\frac{M \vdash G \rightarrow F \quad M \vdash G}{M \vdash F}$$

Korrektheit und Vollständigkeit

Mit dem Kalkül C kann eine Formel φ aus WB abgeleitet werden:

$$WB \vdash_C \varphi.$$

*C ist **korrekt**:*

$$\text{Wenn } WB \vdash_C \varphi, \text{ dann } WB \models \varphi.$$

Die Korrektheit von C folgt aus der Korrektheit der Inferenzregeln.

*C ist **vollständig**:*

$$\text{Wenn } WB \models \varphi, \text{ dann } WB \vdash_C \varphi.$$

Korrektheit des Hilbert-Kalküls

Korrektheit: Sei F eine beliebige aussagenlogische Formel, M eine Menge von Formeln und es gelte $M \vdash F$. Dann folgt daraus auch $M \models F$.

*Beweis über strukturelle
Induktion*

Vorüberlegungen zum Vollständigkeitsbeweis

Wir wollen zeigen: Aus $M \models F$ folgt $M \vdash F$. Wie soll das funktionieren?

- Induktion über die Ableitung?

\rightsquigarrow es gibt gar keine Ableitung!

- Induktion über den Formelaufbau?

Wir müssten beispielsweise beim Induktionsanfang für eine atomare Formel A zeigen:

$$M \models A, \text{ daraus folgt } M \vdash A.$$

Wie kann man eine Ableitung von A aus M konstruieren?

- Weitere Möglichkeiten?

Vollständigkeit (Beweisskizze I)

- (1) Es gilt $M \models F$, genau dann, wenn $M \cup \{\neg F\}$ unerfüllbar ist.
- (2) **Definition (Inkonsistente Formelmeng):** M heißt *inkonsistent*, wenn es eine Formel F gibt mit $M \vdash F$ und $M \vdash \neg F$.
- (3) Es gilt $M \vdash F$, genau dann, wenn $M \cup \{\neg F\}$ inkonsistent ist. (Noch zu beweisen!)
- (4) Jede unerfüllbare Formelmeng ist inkonsistent. Äquivalent dazu: Jede konsistente Formelmeng ist erfüllbar. (Noch zu beweisen!)

Dann gilt: Aus $M \models F$ folgt $M \cup \{\neg F\}$ unerfüllbar. Daraus folgt $M \cup \{\neg F\}$ inkonsistent. Und daraus folgt $M \vdash F$.

Im folgenden zeigen wir (3) & (4), insbesondere: "Jede konsistente Formelmeng ist erfüllbar." (**Trick:** Wir schließen wieder von syntaktischen auf semantische Begriffe.)

Vollständigkeit (Beweisskizze II)

Identifikation von einander entsprechenden Konzepten auf semantischer Seite und auf der Seite des Kalküls:

Semantische Seite	Kalkül
$M \models F$	$M \vdash F$
Unerfüllbarkeit	Inkonsistenz
$M \cup \{F\} \models G$ gdw. $M \models F \rightarrow G$	Deduktionstheorem

Konsistenz

Definition: Eine Menge M von Formeln heißt *konsistent*, falls es keine Formel F gibt, für die sowohl $M \vdash F$ als auch $M \vdash \neg F$ gilt.

Die Menge M heißt *inkonsistent*, falls sie nicht konsistent ist.

Eine Menge M von Formeln heißt *maximal konsistent*, falls sie konsistent ist und für jede Formel F gilt: $F \in M$ oder $\neg F \in M$.

Beispiel – Inkonsistente Mengen

- $M_1 = \{A, \neg A\}$
- $M_2 = \{\neg(A \rightarrow (B \rightarrow A))\}$
- $M_3 = \{\neg B, \neg B \rightarrow B\}$
- $M_4 = \{C, \neg(\neg C \rightarrow D)\}$

Vorüberlegung: Konsistenz/Erfüllbarkeit

Wie zeigt man folgende Aussage?

Wenn M **konsistent** ist, dann ist M **erfüllbar**.

Antwort: Konstruktion einer erfüllenden Belegung \mathcal{A} .

Wenn $A \in M$ gilt, dann setzen wir $\mathcal{A}(A) = 1$.

Wenn $\neg A \in M$ gilt, dann setzen wir $\mathcal{A}(A) = 0$.

Problem: Was macht man, wenn weder $A \in M$, noch $\neg A \in M$ gilt?

Antwort: Das kann bei maximal konsistenten Mengen nicht vorkommen! Wir erweitern M daher zunächst zu einer maximal konsistenten Menge \overline{M} .

Aufzählung aller Formeln

Wie konstruiert man eine **Aufzählung** F_1, F_2, F_3, \dots aller Formeln?
Die genaue Reihenfolge ist dabei unwichtig!

for $i = 1, 2, 3, \dots$ **do**

 Gebe alle Formeln der Länge kleiner gleich i , die nur atomare
 Formeln der Form $A_j, j \leq i$ enthalten, aus.

 Bereits früher erzeugte Formeln werden nicht ausgegeben.

end

Dies ergibt beispielsweise folgende Aufzählung:

$$\underbrace{A_1}_{i=1}, \underbrace{A_2, \neg A_1, \neg A_2}_{i=2}, \underbrace{A_3, \neg A_3, A_1 \vee A_2, A_1 \vee A_3, \dots}_{i=3}, \dots$$

Vollständigkeit

Vollständigkeit: Sei F eine beliebige aussagenlogische Formel, M eine Menge von Formeln und es gelte $M \models F$. Dann folgt daraus auch $M \vdash F$.

Nachbemerkungen

- Die Axiome (4) und (5) sind nicht unbedingt notwendig, sie können aus den anderen drei Axiomen hergeleitet werden.
- Es gibt auch einen Hilbert-Kalkül für die Prädikatenlogik!

Endlichkeitssatz

Der **Endlichkeitssatz** kann mit Hilfe des **Vollständigkeitsresultats** bewiesen werden.

Zu zeigen: Wenn jede endliche Teilmenge von M erfüllbar ist, dann ist auch M erfüllbar.

Angenommen, M wäre unerfüllbar. Dann ist M inkonsistent (siehe Vollständigkeitsbeweis), d.h., es gilt $M \vdash F$ und $M \vdash \neg F$ für eine Formel F . In diesen Ableitungen können nur endlich viele Hypothesen aus M verwendet werden, d.h., es gibt eine endliche Teilmenge $M' \subseteq M$ mit $M' \vdash F$ und $M' \vdash \neg F$. Die Menge M' ist also inkonsistent und damit unerfüllbar (Übungsaufgabe). Das ist aber ein Widerspruch zur Voraussetzung.

Kompaktheit

- Eine Logik, für die der Endlichkeitssatz gilt, wird auch kompakt genannt.

Herbrand-Universum

Das *Herbrand-Universum* $D(F)$ einer geschlossenen Formel F in Skolemform ist die Menge aller variablenfreie Terme, die aus den Bestandteilen von F gebildet werden können. Im speziellen Fall, daß in F keine Konstante vorkommt, wählen wir zunächst eine beliebige Konstante, zum Beispiel a , und bilden dann die variablenfreien Terme. Formaler ausgedrückt, $D(F)$ wird wie folgt induktiv definiert:

- (1) Alle in F vorkommenden Konstanten sind in $D(F)$. Falls F keine Konstante enthält, so ist a in $D(F)$.
- (2) Für jedes in F vorkommende n -stellige Funktionssymbol f und Terme t_1, t_2, \dots, t_n in $D(F)$ ist der Term $f(t_1, t_2, \dots, t_n)$ in $D(F)$.

Jacques Herbrand 1908-1931

Herbrand-Strukturen

Sei F eine Aussage in Skolemform. Dann heißt jede zu f passende Struktur $\mathcal{A} = (U_{\mathcal{A}}, I_{\mathcal{A}})$ eine *Herbrand-Struktur* für F , falls folgendes gilt:

- (1) $U_{\mathcal{A}} = D(F)$,
- (2) für jedes in F vorkommende n -stellige Funktionssymbol f und $t_1, t_2, \dots, t_n \in D(F)$ ist $f^{\mathcal{A}}(t_1, t_2, \dots, t_n) = f(t_1, t_2, \dots, t_n)$.

Der fundamentale Satz der Prädikatenlogik

Satz: Sei F eine Aussage in Skolemform. F ist genau dann erfüllbar, wenn F ein Herbrand-Modell besitzt.

Herbrand-Expansion

Sei $F = \forall y_1 \forall y_2 \dots \forall y_n F^*$ eine Aussage in Skolemform. Dann ist $E(F)$ die *Herbrand-Expansion* von F , definiert als

$$E(F) = \{F^*[y_1/t_1][y_2/t_2] \dots [y_n/t_n] \mid t_1, t_2, \dots, t_n \in D(F)\}$$

Die Formeln in $E(F)$ entstehen also, indem die Terme in $D(F)$ in jeder möglichen Weise für die Variablen in F^* substituiert werden.

Satz von Gödel–Herbrand–Skolem

Satz: Für jede Aussage F in Skolemform gilt: F ist erfüllbar genau dann, wenn die Formelmenge $E(F)$ (im aussagenlogischen Sinn) erfüllbar ist.

Beweis: Es genügt zu zeigen, daß F ein Herbrand-Modell besitzt genau dann, wenn $E(F)$ erfüllbar ist.

Die Formel F habe die Form $\forall y_1 \forall y_2 \dots \forall y_n F^*$. Nun gilt:

\mathcal{A} ist ein Herbrand-Modell für F
gdw. für alle $t_1, t_2, \dots, t_n \in D(F)$ gilt:

$$\mathcal{A}_{[y_1/t_1][y_2/t_2]\dots[y_n/t_n]}(F^*) = 1$$

gdw. für alle $t_1, t_2, \dots, t_n \in D(F)$ gilt:

$$\mathcal{A}(F^*[y_1/t_1][y_2/t_2] \dots [y_n/t_n]) = 1$$

gdw. für alle $G \in E(F)$ gilt $\mathcal{A}(G) = 1$

gdw. \mathcal{A} ist ein Modell für $E(F)$

Satz von Herbrand

Satz: Eine Aussage F in Skolemform ist unerfüllbar genau dann, wenn es eine endliche Teilmenge von $E(F)$ gibt, die (im aussagenlogischen Sinn) unerfüllbar ist.

Beweis: Ummittelbare Folge des Satzes von Gödel-Herbrand-Skolem und des Endlichkeitssatzes.

Algorithmus von Gilmore

Sei F eine prädikatenlogische Aussage in Skolemform und sei $\{F_1, F_2, F_3, \dots, \}$ eine Aufzählung von $E(F)$.

Eingabe: F

$n := 0$;

repeat $n := n + 1$;

until $(F_1 \wedge F_2 \wedge \dots \wedge F_n)$ ist unerfüllbar;

Gib "unerfüllbar" aus und stoppe.

Satz von Löwenheim–Skolem

1915

Satz: Jede erfüllbare Formel der Prädikatenlogik besitzt bereits ein abzählbares Modell (also eines mit abzählbarer Grundmenge).

Beweis: Aus F gewinnen wir G in Skolemform mit:

F hat ein Modell mit Grundmenge X genau dann, wenn G ein Modell mit Grundmenge X hat.

F erfüllbar $\rightarrow G$ erfüllbar $\rightarrow G$ besitzt ein **Herbrand**-Modell (X, I_1)
 $\rightarrow F$ besitzt ein Modell (X, I_2) $\rightarrow F$ besitzt ein abzählbares Modell
(da X aufzählbar)

Albert Thoralf Skolem 1887-1963

Leopold Löwenheim 1878-1957

Resümee

- Korrektheit und Vollständigkeit für Algorithmen
 - ◆ hier ist besonders auch Terminierung interessant
 - ◆ Entscheidbarkeit (gibt es Algorithmen?)
- Korrektheit und Vollständigkeit für Axiomensysteme
 - ◆ Endlich axiomatisierbar?
 - ◆ Terminierung nicht/weniger relevant

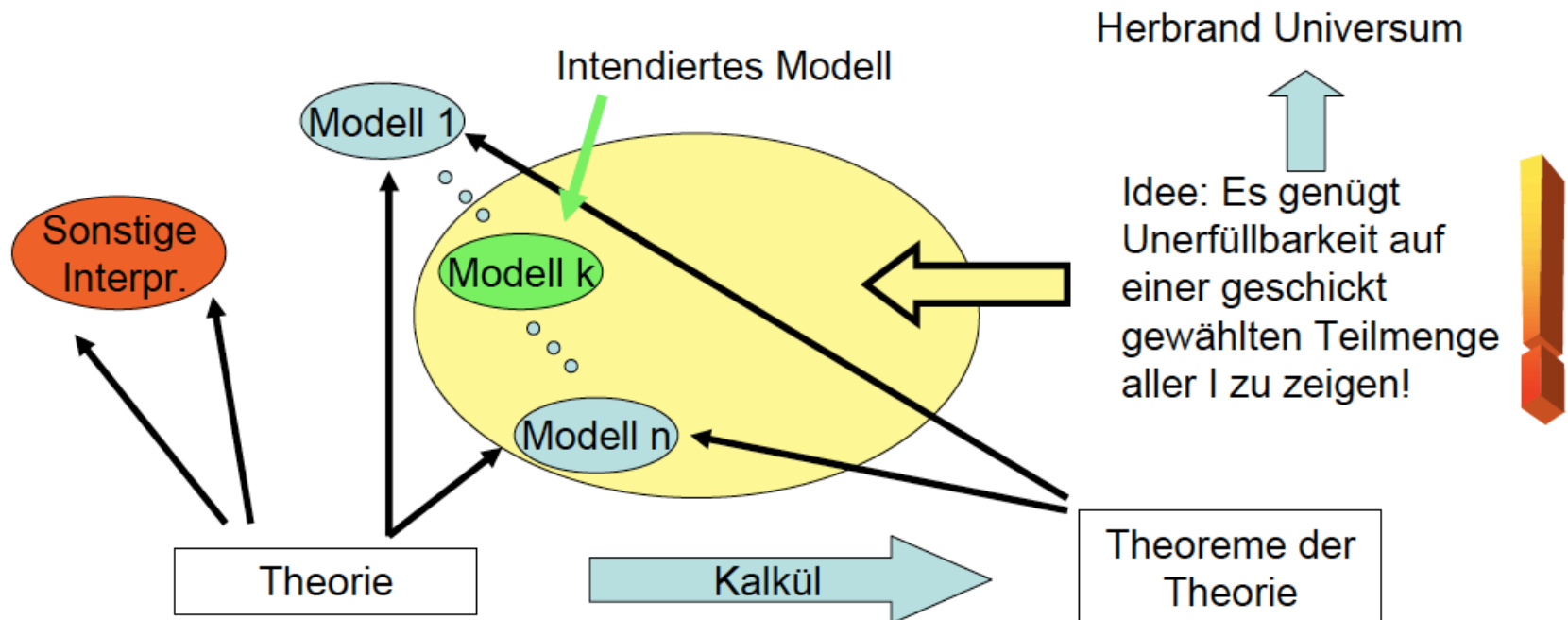
Hilbert-Programm

- David Hilbert
- Ziel: Aufbau der Arithmetik (und damit der ganzen Mathematik) auf widerspruchsfreiem Axiomensystem (ca. 1920)
- Erwies sich als undurchführbar (Gödelscher Unvollständigkeitssatz, 1930)

Beweistheorie vs. Modelltheorie

- Beweistheoretische Sicht:
 - ◆ Führe Axiome (nicht Axiomenschemata) ein, so dass gewünschte Beweise möglich werden und andere nicht
- Modelltheoretischen Sicht:
 - ◆ Führe Axiome ein, um die Modelle zu reduzieren und nicht-intendierte Modelle zu eliminieren

Macht und Ohnmacht...



Modelltheorie

- Alfred Tarski
 - ◆ Polnisch-US-amerikanischer Mathematiker und Logiker
- Einführung der modelltheoretischen Semantik (1936)
- Formale Definition von Entscheidungsproblemen
- Prägung der Mathematischen Logik (1937)

Logische Modellierung

- Aufstellen von Formeln (Axiome)
- Formulierung von Anwendungsproblem als Entscheidungs- oder Berechnungsproblem
- OWA, no UNA, no DCA

Beweissysteme

- Hilbert–Kalküle
 - ◆ Axiomenschemata + Inferenzregel (Modus Ponens)
 - ◆ Folgerungsbeweis
 - Herleitung der gesuchten Formel
- Resolution
 - ◆ Erfüllbarkeitstester
 - Herleitung der leeren Klausel (Widerspruch)
- Tableau–Beweiser
 - ◆ Erfüllbarkeitstester / Konsistenztester
 - Systematische Konstruktion eines (kanonischen Modell)

Es dreht sich mittlerweile alles um Modelle

- Aussagenlogik
 - ♦ Belegung (“Bitvektor”)
- Prädikatenlogik
 - ♦ Relationale Struktur
 - ♦ Interpretation
 - ♦ Herbrand Modell
(nach Jacques Herbrand)
- Temporale Logik
 - ♦ Zeitstrukturen (linear, baumförmig)
- Modallogik: Logik der erreichbaren Zustände
 - ♦ Kripke-Strukturen (Graphen)

Und so ging's weiter ...

- before 1950: Proof-theoretic Work by Skolem, Herbrand, Gentzen and Schütte
- 1954: First machine-generated Proof (Davis)
- 1955ff: Semantic Tableaus (Beth, Hintikka)
- 1957: First machine-generated Proof in Logic Calculus (Newell & Simon)
- 1957: Lazy substitution by free (dummy) Vars (Kanger, Prawitz)
- 1958: First prover for Predicate Logic (Prawitz)
- 1959: More provers (Gilmore, Wang)
- 1960: Davis-Putnam Procedure (Davis, Putnam, Longman)
- 1963: Unification (J.A. Robinson)
- 1963ff: Resolution (J.A. Robinson); Inverse Method (Maslov)
- 1963ff: Modern Tableau Method (Smullyan, Lis) without Unification
- 1968: Model elimination (Loveland), with Unification
- 1970ff: PROLOG (Colmerauer, Kowalski), Refinements of Resolution
- 1971: Cook, NP-Completeness for SAT
- 1971: Connection Method (Bibel), Matings (Andrews) with Unification
- 1977: Dependency-directed Backtracking (Stallman, Sussman)
- 1985: ATP in non-classical logics, Renaissance of Tableaux Methods
- 1987: Tableaus with Unification
- 1993ff: Renewed interest in Instance-based Methods: DPLL, Model evolution
- 1995: Heuristics (Freeman)
- 1996ff: Praktisch einsetzbare Beschreibungslogikbeweiser
- ...

...mit der Zeit

- 1970: LTL (Pnueli, Manna)
- 1980: CTL (Clarke, Emerson)
- 1986: CTL* (Emerson, Halpern)
- 1990: Symbolic Model Checking (McMillan)
- 1991: SPIN for LTL (Holzman)
- 1993: SMV for CTL (McMillan)
- ...