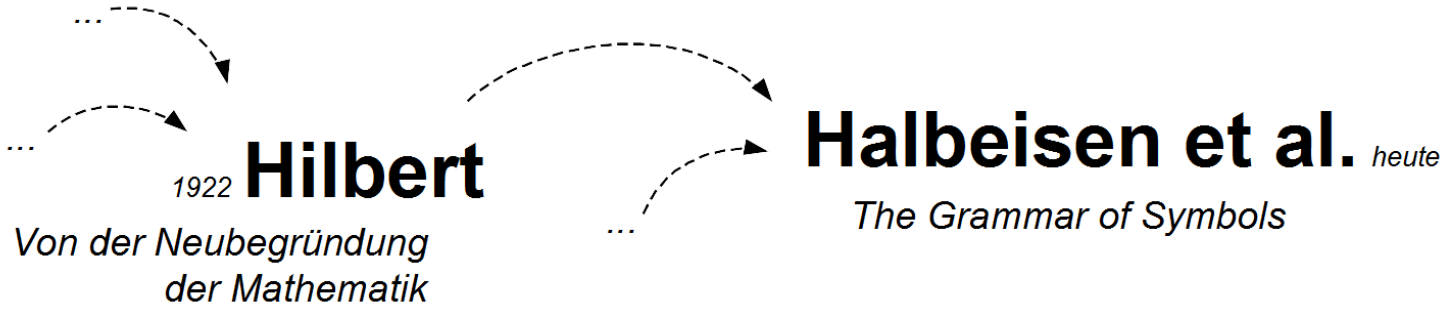
Hilbert: Prädikatenlogik Teil I (formale Beweise)

Text von Hilbert; Text von Halbeisen et al.



Christine Simantiri
Ueli Gisiger
13.04.2016

Hilbert: Prädikatenlogik Teil I (formale Beweise)

Ablauf der Text-Vorstellung

1. Hilbert und die Krise
2. Hilbert
3. Fragen und Diskussion

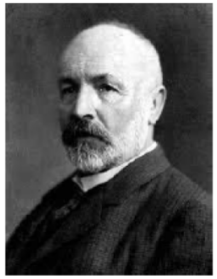
-- Pause --

4. Halbeisen et al. Formales
5. Halbeisen et al. Semi-Formales
6. Fragen und Diskussion

Die Logiker-Krise

L. Kronecker

Ablehnung der Mengenlehre, "Abschaffung " der irrationalen Zahl "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk"



G. Cantor

Axiomatische Mengenlehre ca. 1899

G. Frege

Versuch die Zahlenlehre auf reine Logik zu begründen, ca. 1879

VS

L. Brouwer

H. Weyl

Es gibt Teufelskreise/Paradoxa in der Mengenlehre. *Intuitionismus* ca.1908

D. Hilbert

Hilbert

Gödel

Halbeisen et al.

pre *post*

1922 | 1931 | 2016 |

Unvollständigkeitssatz

David Hilbert

1895: Professor an der Universität von Göttingen

1900: Stellung der 23 Probleme beim 2.ten internationalen Mathematikerkongress in Paris

1943: Tod in Göttingen

Geboren 1862 in Königsberg

1899: Veröffentlichung von "Grundlagen der Geometrie"

1922: "Neubegründung der Mathematik"

"Wir dürfen nicht denen glauben, die heute mit philosophischer Miene und überlegenem Tone den Kulturuntergang prophezeien und sich in dem Ignorabimus gefallen. Für uns gibt es kein Ignorabimus, und meiner Meinung nach auch für die Naturwissenschaft überhaupt nicht. Statt des törichten Ignorabimus heiße im Gegenteil unsere Lösung:
Wir müssen wissen, Wir werden wissen."

aus Hilbert's Vortrag "Naturerkennen und Logik", 1930

Alphabet

ZAHLENTHEORIE

1 ist eine Zahl, damit auch alle Zeichen bestehend aus 1 und +, z.B. 1+1

1+1+1

Diese Zahlzeichen machen die ganzen Zahlen vollständig aus, haben aber keine *Bedeutung*. Ausserdem führen wir zur Abkürzung die folgenden Zeichen die etwas *bedeuten*: 2=1+1

3=1+1+1

Ferner werden wir auch die Symbole =,> benutzen, die zur Mitteilung von Behauptungen dienen.

Keine Axiome => Keine Widersprüche möglich!

GRUNDLAGEN DER MATHEMATIK

I. Individualzeichen

1. 1,+ (Bestadteile der Zahlzeichen)
2. $\phi(*)$, $\psi(*)$ (individuelle Funktionen)
3. =,+,>
4. Z (Zahl sein), Φ (Funktion sein)
5. $\longrightarrow$ ("folgt", logisches Zeichen)
6. ( ) (Allzeichen)

II. Variable

1. a,b,c,d (Grundvariable)
2. f(*),g(*,*) (variable Funktionen)
3. A,B,C,D (variable Formeln)

III. Zeichen zur Mitteilung

1. $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ (Funtktionale)
2. $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{G}, \mathfrak{L}$ (Formeln)

- Ein *Funktional* ist ein Zahlzeichen/Grundvariable/Funktion, deren Leerstellen mit Zahlzeichen/Grundvariablen/Funktionen ausgefüllt sind.
- Wenn man an beiden Seiten eines Folgezeichens ein Funktional setzt, dann entsteht eine *Folgeformel*.

Axiome und Beweise

Definition: Formeln, die als Bausteine des formalen Gebäudes der Mathematik dienen, werden *Axiome* genannt.

1. $a=a$
2. $1+(a+1)=(1+a)+1$
3. $a=b \longrightarrow a+1=b+1$
4. $a+1=b+1 \longrightarrow a=b$
5. $a=c \longrightarrow (b=c \longrightarrow a=b)$

Definition: Ein *Beweis* ist eine Figur, die uns als solche anschaulich vorliegen muss ; er besteht aus Schussfolgerungen vermöge des Schlußschemas:

$$\frac{\mathcal{G} \qquad \mathcal{G} \longrightarrow \mathcal{L}}{\mathcal{L}}$$

wobei jede der Prämissen ein Axiom ist, oder direkt durch das Einsetzen eines Axioms entsteht. Dementsprechend ist eine Formel *beweisbar*, wenn sie entweder ein Axiom ist, oder die Endformel eines Beweises ist.

Beweise werden selbst als Gegenstände unserer Untersuchung betrachtet, dadurch entsteht eine sogenannte *Beweistheorie*.

Widerspruchsfreicheit

• "beweisbar" ist immer relativ bezüglich des definierten Axiomensystems zu verstehen, d.h. beide 1=1 und 1=1+1 könnten als Formeln gelten.

• Damit der hier eingeführte Formalismus die wirkliche mathematische Theorie völlig bedient, muss ein Analogon für den Widerspruch eingeführt werden.

Definition: Ein Axiomensystem ist *widerspruchsfrei*, wenn in diesem

$a=b$ und $a\neq b$

niemals gleichzeitig beweisbar sind, wobei a,b Funktionale sind.

Ersetzen des 2. Axioms (1+(a+1)=(1+a)+1) durch das folgende:

6. a+1 ≠ 1

Hauptziel

SATZ: Das Axiomensystem, das aus den fünf Axiomen

1. $a=a$
3. $a=b \longrightarrow a+1=b+1$
4. $a+1=b+1 \longrightarrow a=b$
5. $a=c \longrightarrow (b=c \longrightarrow a=b)$
6. $a+1 \neq 1$

besteht, ist widerspruchsfrei.

Vervollständigung des Axiomensystems

- Die bis jetzt angegebenen Axiome machen nur einen kleinen Teil der Arithmetik aus und bilden noch keine Grundlage für die Theorie der reellen Zahl.
- Dazu kommen weitere Axiome, u.a. das der *vollständigen Induktion*, Axiome des logischen Schließens und weitere arithmetische Axiome.

Wie macht man also weiter?

1. Man müsste formale Logik und Arithmetik gleichzeitig aufbauen, da deren Grundlagen in enger Beziehung stehen.
2. Neue Formeln werden aus den bereits erworbenen Axiomen erzeugt und neue Axiome werden hinzugefügt.

!!! Widerspruchsfreiheit des Axiomensystems muss immer geprüft werden.

Hilbert

Fragen zu Hilbert

Q1

Hat Hilbert sein Ziel erreicht?

Hilbert: Prädikatenlogik Teil I (formale Beweise)

Jetzt ...

Pause!

Halbeisen et al.

Syntax – Alphabet

Logische Symbole

- *Variablen* $x, y, v_0, v_1, \ldots,$
- *Logische Operatoren* "$\neg$" (*not*), "$\wedge$" (*and*), "$\vee$" (*or*), and "$\rightarrow$" (*implies*).
- *Logische Quantifikatoren* "$\exists$" Existenz, "$\forall$" All-Quantor
- *Gleichheitssymbol* "$=$" Gleichheitsrelation

Nicht-logische Symbole (domänenspezifisch)

- *Konstanten Symb.* *fixierte individuelle Objekte der Domäne, "e"*
- *Funktionen Symb.* *Obj. als Argument/Rückgabe, Wertigkeit, "$\circ$"*
- *Relationen Symb.* *Relationen zwischen Dom.Obj., "R x x x"*

Sprache/Signatur:

Endliche Menge an "Nicht logischen Symbolen"

Bsp: Group Theory: $\mathscr{L} = \{\mathbf{e}, \circ\}$

Halbeisen et al.

Syntax – Worte und Sätze

Term als Zeichenkette von Symbolen (Regeln T0-T2)

- *T0 jedes variablen, T1 jedes konstanten Symbol*
- *Bsp: T2* $F\tau_1 \cdots \tau_n$ is a term

Formulae als Zeichenkette von Symbolen

- *atomare Formulae (Regeln F0-F1)*

(F0) If τ_1 and τ_2 are terms, then $\tau_1 = \tau_2$ is a formula.

(F1) If $\tau_1, \ldots, \tau_n$ are any terms and $R\mathsf{x}\cdots\mathsf{x}$ is any non-logical n-ary relatio symbol, then $R\tau_1 \cdots \tau_n$ is a formula.

- *weitere (Regeln F2-F4)*
  Bsp: F4

(F4) If φ is a formula which we have already built, and ν is an arbitrary variable, then $\exists\nu\varphi$ and $\forall\nu\varphi$ are formulae.

Halbeisen et al.

Syntax – Axiome und Theorie

Axiome als wahre Formulae

- *Logisches Axiom: universal gültige Formulae*
- *Axiom Schema*

L_0: $\varphi \vee \neg\varphi$,

L_1: $\varphi \to (\psi \to \varphi)$,

L_2: $(\psi \to (\varphi_1 \to \varphi_2)) \to ((\psi \to \varphi_1) \to (\psi \to \varphi_2))$,

...

- *Nicht logische Axiome*

Theorie als Menge von nicht-logischen Axiomen

GT_0: $\forall x \forall y \forall z (x \circ (y \circ z) = (x \circ y) \circ z)$ (*i.e.*, "$\circ$" is *associative*)

GT_1: $\forall x (\mathsf{e} \circ x = x)$ (*i.e.*, "e" is a *left-neutral* element)

...

Halbeisen et al.
Inferenz und Formaler Beweis

Inferenzregeln

MODUS PONENS (MP): $\dfrac{\varphi \to \psi,\ \varphi}{\psi}$ GENERALISATION ($\forall$): $\dfrac{\varphi}{\forall \nu \varphi}$.

Formaler Beweis

- *X-Sprache (Menge von nicht-logischen Symbolen)*
- *T eine X-Theorie (Menge von nicht-logischen Axiomen)*
- *X-Formulae ψ ist beweisbar in T, wenn:*
  Sequenz "φ0, . . . , φn" von X-Formulae, sodass φn ≡ ψ" $\mathsf{T} \vdash \psi$
  - φ_i is a logical axiom, or
  - $\varphi_i \in \mathsf{T}$, or
  - there are $j, k < i$ such that $\varphi_j \equiv \varphi_k \to \varphi_i$, or
  - there is a $j < i$ such that $\varphi_i \equiv \forall \nu\, \varphi_j$ for some variable ν.

Wenn ψ in T nicht beweisbar: $\mathsf{T} \nvdash \psi$

Halbeisen et al.
Inferenz und Formaler Beweis

formal proof of $\varphi \to \varphi$

φ_0:	$(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$	instance of L_2
φ_1:	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	instance of L_1
φ_2:	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	from φ_0 and φ_1 by (MP)
φ_3:	$\varphi \to (\varphi \to \varphi)$	instance of L_1
φ_4:	$\varphi \to \varphi$	from φ_2 and φ_3 by (MP)

φ0: (φ → ((φ → φ) → φ)) → ((φ → (φ → φ)) → (φ → φ))

- *Axiom Schema L2:*
  (ψ → (φ1 → φ2)) → ((ψ → φ1) → (ψ → φ2))

- *Instanziieren mit: ψ als φ; φ1 als φ → φ; φ2 als φ;*

- *Logisches Axiom*

φ0: (φ → ((φ → φ) → φ)) → ((φ → (φ → φ)) → (φ → φ))

Halbeisen et al.
Semi-formale Beweise

Stand
- *... zu motivieren*

Ziel
- *Lesbarkeit erhöhen*
- *Text präzise formal definieren*
- *(kontrollierte) natürliche Sprache als Input für formale Beweise*
- *Übersetzung in formalen Beweis*
- *Verifikation durch Beweis-Prüf-System*

Mittel
- *(kontrollierte) natürliche Sprache*
- *Limitiertes Vokabular*
- *Phrasen, häufig in mathematischen Beweis-Texten verwendet*

Halbeisen et al.

Semi-formale Beweise

Operationen auf Targets (Backward reasoning)

- *„Assume ... Then ... This shows ...“*
- *„Suppose for a contradiction that .... Then ... Contradiction“*
- *„We proceed by contraposition... This shows ...“*

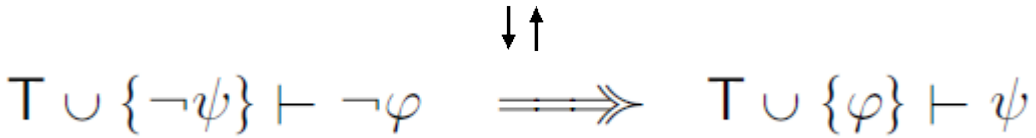
Operationen auf Prämissen (Forwards reasoning)

- *„We show first ... This proves ...“*
- *„This shows/proves ...“*

Halbeisen et al.

Semi-formale Beweise & Art of Proof

„We proceed by contraposition... This shows ¬φ“



Die Kunst des Beweisens: Formale Beweise vereinfachen

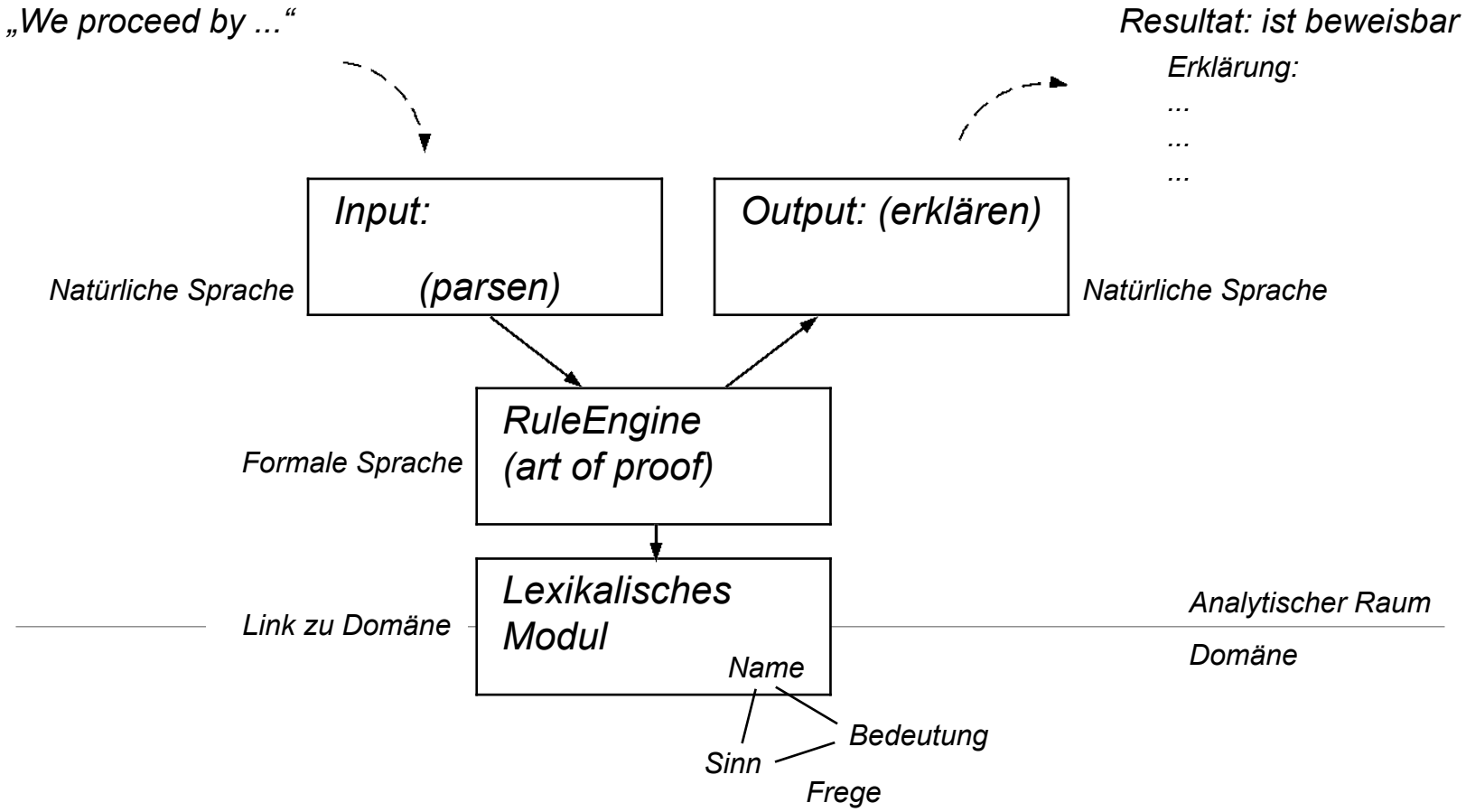
- *aus "φ ∧ ψ" wird "φ beweisen; ψ beweisen; wenn beide beweisbar, dann ist 'φ ∧ ψ' bewiesen"*
- *case distinctions*
- *proof by contradiction*

Verständnis:

- *Beweismethoden als Operationen auf endlichen Listen von Goals aus Prämissen und Target*

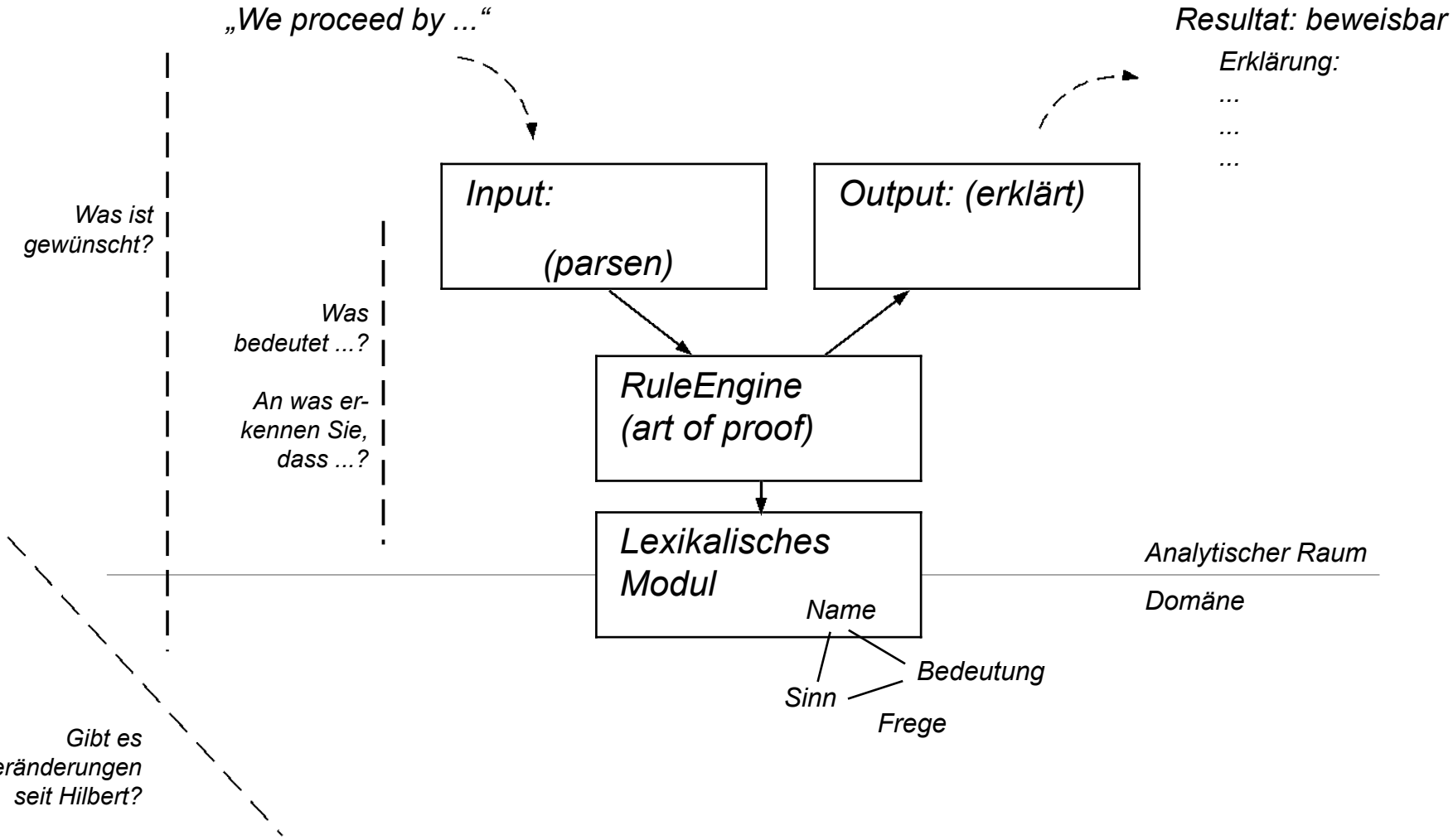
Halbeisen et al.

... hin zum Expertensystem – Q2?



Halbeisen et al.

... normative Rahmungen – Q3?



Hilbert: Prädikatenlogik Teil I (formale Beweise)

Zum Schluss ...

Besten Dank!