Logik für Informatiker

Viorica Sofronie-Stokkermans

e-mail: sofronie@uni-koblenz.de

Logik in der Informatik

Was ist Logik?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

- Unverständlich?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

- Unverständlich?

- Reine Theorie ohne praktischen Nutzen?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

  ja

- Unverständlich?

- Reine Theorie ohne praktischen Nutzen?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

  ja

- Unverständlich?

  hoffentlich nein

- Reine Theorie ohne praktischen Nutzen?

Logik in der Informatik

Was ist Logik?

- Mathematisch?

  ja

- Unverständlich?

  hoffentlich nein

- Reine Theorie ohne praktischen Nutzen?

  nein: Verifikation von Hardware, Software, Protokollen

  Sprachverarbeitung und Wissensrepräsentation

  Abfragensprachen für Datenbanken; ...

Formale Logik

Ziel

- Formalisierung und Automatisierung rationalen Denkens
- Rational richtige Ableitung von neuem Wissen aus gegebenem

Rolle der Logik in der Informatik

- Anwendung innerhalb der Informatik
  Spezifikation, Programmentwicklung, Programmverifikation
- Werkzeug für Anwendungen außerhalb der Informatik
  Künstliche Intelligenz, Wissensrepräsentation

Formale Logik

Ziel

- Formalisierung und Automatisierung rationalen Denkens
- Rational richtige Ableitung von neuem Wissen aus gegebenem

Rolle der Logik in der Informatik

- Anwendung innerhalb der Informatik
  Spezifikation, Programmentwicklung, Programmverifikation
- Werkzeug für Anwendungen außerhalb der Informatik
  Künstliche Intelligenz, Wissensrepräsentation

Modellierung

Modellierung

Abstraktion

Modellierung

Abstraktion

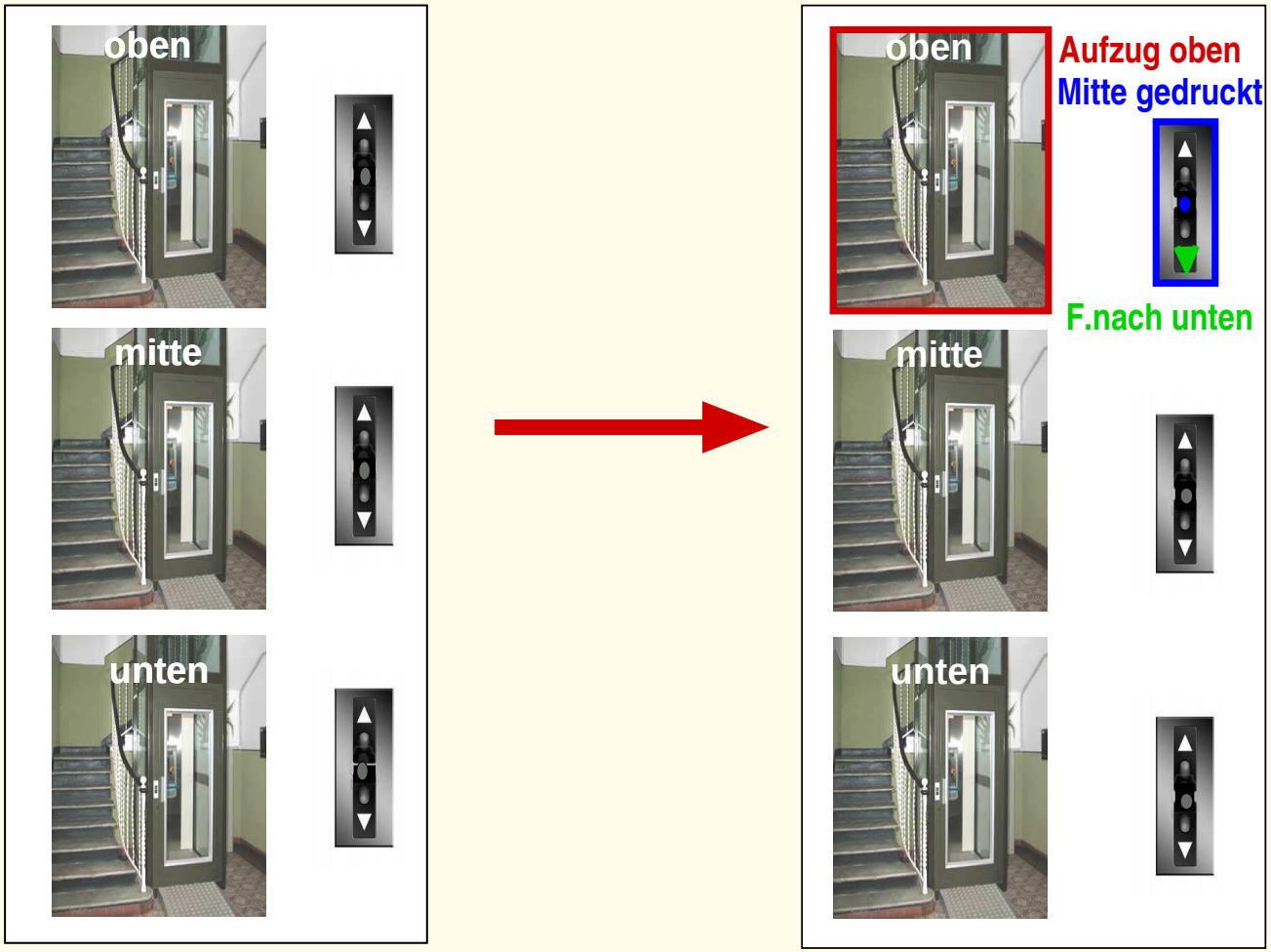
Modellierung

Adäquatheit des Modells

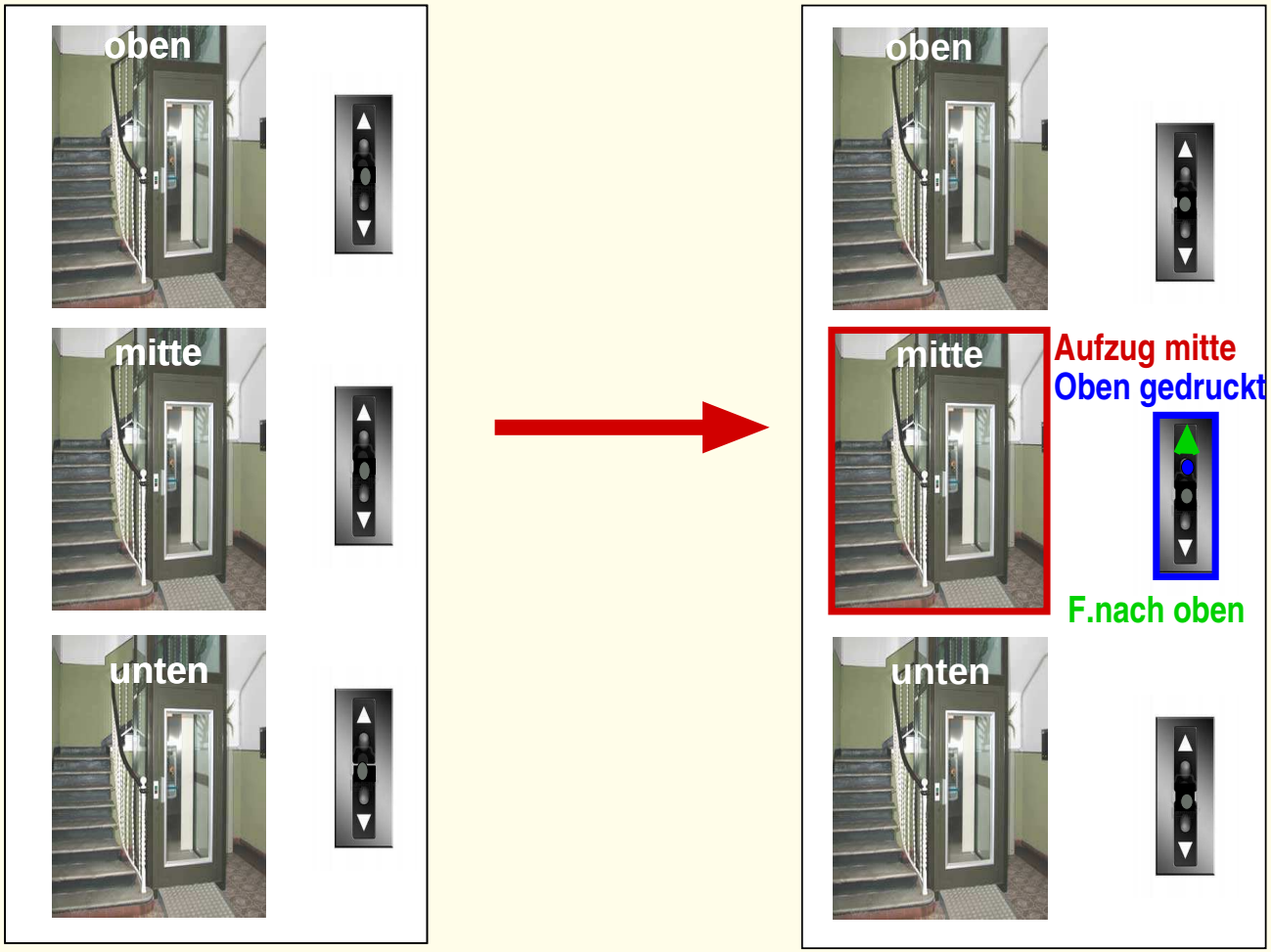
Wenn formulierbare Aussage wahr im Modell, dann entsprechende Aussage wahr in Wirklichkeit

Beispiel: Aufzug

Beispiel: Aufzug



Beispiel: Aufzug



Modellierung: Strukturen

v(AufzugOben) = wahr

v(MitteGedrückt) = wahr

v(FährtNachUnten) = wahr

v(AufzugMitte) = wahr

v(UntenGedrückt) = wahr

v(FährtNachUnten) = wahr

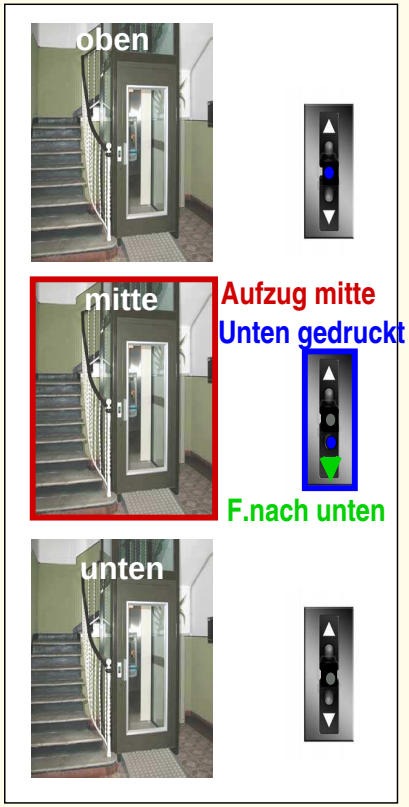
v(AufzugOben) = wahr

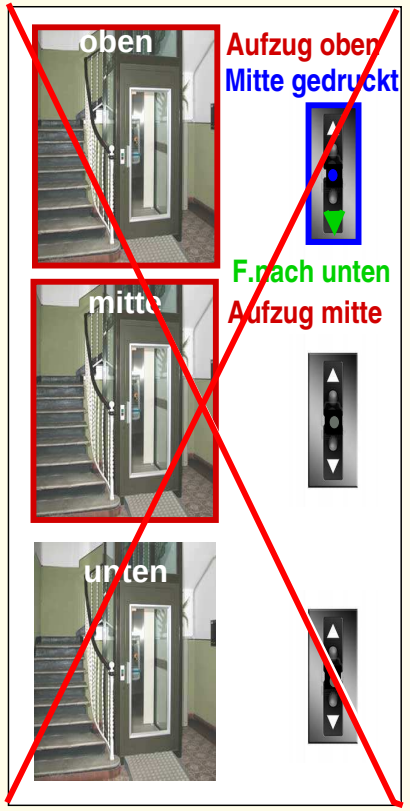
v(AufzugMitte) = wahr

v(MitteGedrückt) = wahr

v(FährtNachUnten) = wahr

Modellierung: Strukturen





v(AufzugOben) = wahr

v(MitteGedrückt) = wahr

v(FährtNachUnten) = wahr

v(AufzugMitte) = wahr

v(UntenGedrückt) = wahr

v(FährtNachUnten) = wahr

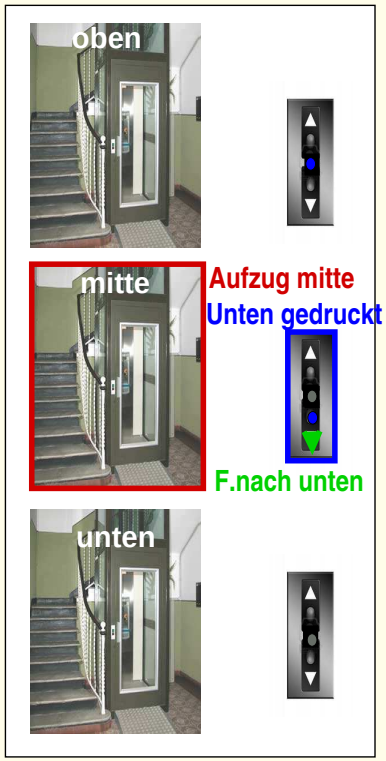
v(AufzugOben) = wahr

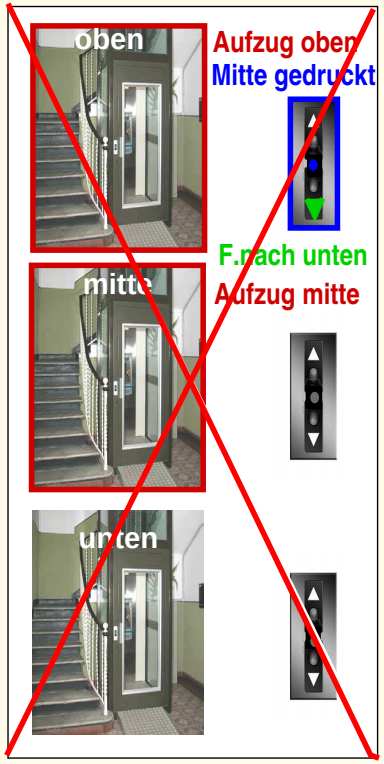
v(AufzugMitte) = wahr

v(MitteGedrückt) = wahr

v(FährtNachUnten) = wahr

Modellierung: Strukturen





Aussagen beziehen sich auf Strukturen

(Formale) Aussagen sind in jeder einzelnen Struktur zu wahr oder falsch auswertbar

Formale Logik

- Syntax

  welche Formeln?

- Semantik

  Modelle (Strukturen)

  Wann ist eine Formel wahr (in einer Struktur)?

- Deduktionsmechanismus

  Ableitung neuer wahrer Formeln

Aussagenlogik

Die Welt besteht aus Fakten

Aussagenlogik: Syntax

Die Welt besteht aus Fakten

Bausteine: Atomare Aussagen

Aussagenlogik: Syntax

Die Welt besteht aus Fakten

Bausteine: Atomare Aussagen

Beispiele: Aufzug ist oben:

AufzugOben

Mittlerer Knopf gedrückt:

MitteGedrückt

Aussagenlogik: Syntax

Die Welt besteht aus Fakten

Bausteine: Atomare Aussagen

Beispiele: Aufzug ist oben:

AufzugOben

Mittlerer Knopf gedrückt:

MitteGedrückt

Verknüpft mit logischen Operatoren

und	oder	impliziert ("wenn, dann")	nicht
$\wedge$	$\vee$	$\rightarrow$	$\neg$

Aussagenlogik: Syntax

Komplexe Aussagen:

Beispiele:

Wenn mittlerer Knopf gedrückt, dann Aufzug nicht in der Mitte

$$\text{MitteGedrückt} \rightarrow \neg\text{AufzugMitte}$$

Der Aufzug ist oben und der Aufzug ist nicht unten

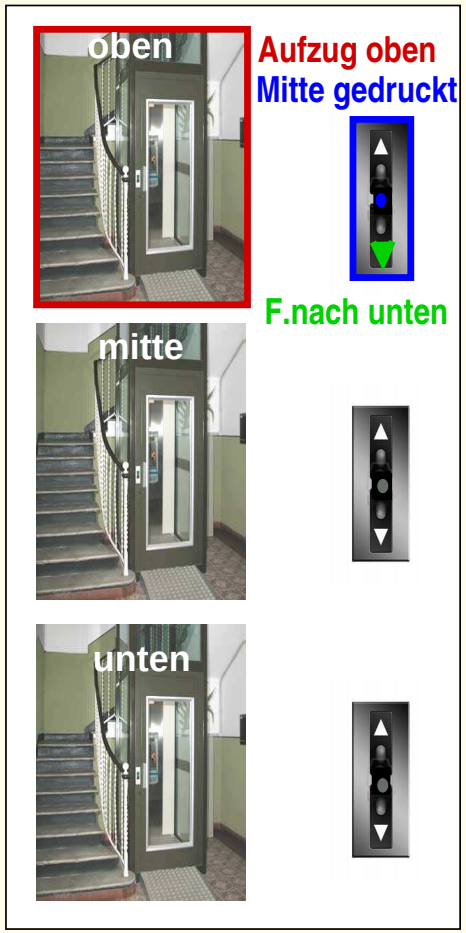
$$\text{AufzugOben} \wedge \quad \neg\text{AufzugUnten}$$

Aussagenlogik: Semantik

Der Aufzug ist oben und der Aufzug ist nicht unten

$$\text{AufzugOben} \wedge \neg\text{AufzugUnten}$$

wahr in:

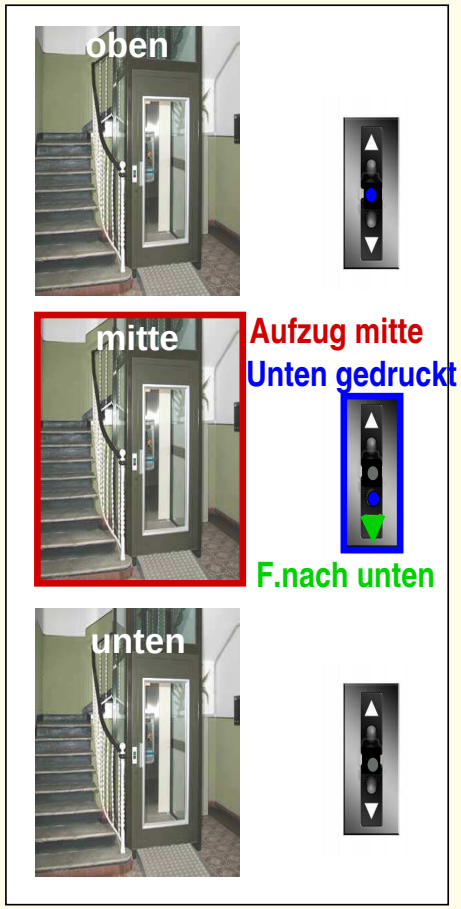


Aussagenlogik: Semantik

Der Aufzug ist oben und der Aufzug ist nicht unten

$$\text{AufzugOben} \wedge \neg\text{AufzugUnten}$$

falsch in:



Aussagenlogik: Deduktionsmechanismus

- Deduktionsmechanismus

  Ableitung neuer wahrer Formeln

Syllogismen:

$$\frac{P \qquad P \rightarrow Q}{Q}$$

Aussagenlogik: Deduktionsmechanismus

- Deduktionsmechanismus

  Ableitung neuer wahrer Formeln

Syllogismen:

$$\frac{P \qquad P \rightarrow Q}{Q}$$

$$\frac{\text{AufzugUnten} \qquad \text{AufzugUnten} \rightarrow \neg\text{AufzugOben}}{\neg\text{AufzugOben}}$$

Aussagenlogik: Deduktionsmechanismus

Deduktionsmechanismus im allgemeinen

Kalkül

In dieser Vorlesung:

- Wahrheitstafeln
- Logische Umformung
- Resolutionskalkül
- Tableaukalkül

Prädikatenlogik

Aussagenlogik: Die Welt besteht aus Fakten

Prädikatenlogik

Aussagenlogik: Die Welt besteht aus Fakten

... aber: Aussagenlogik hat nur beschränkte Ausdruckskraft

Prädikatenlogik

Aussagenlogik: Die Welt besteht aus Fakten

... aber: Aussagenlogik hat nur beschränkte Ausdruckskraft

Beispiele:

- Die Aussage “Alle Menschen sind sterblich” erfordert eine Formel für jeden Mensch.
- Die Aussage “Jede natürliche Zahl ist entweder gerade oder ungerade” erfordert eine Formel für jede Zahl.

Prädikatenlogik

Reichere Struktur

- Objekte (Elemente)
  Leute, Häuser, Zahlen, Theorien, Farben, Jahre, ...

Prädikatenlogik

Reichere Struktur

- Objekte (Elemente)
  Leute, Häuser, Zahlen, Theorien, Farben, Jahre, ...
- Relationen/Eigenschaften
  rot, rund, gerade, ungerade, prim, mehrstöckig, ...
  ist Bruder von, ist größer als, ist Teil von, hat Farbe, besitzt, ..
  $=$, $\geq$, ...

Prädikatenlogik

Reichere Struktur

- Objekte (Elemente)
  Leute, Häuser, Zahlen, Theorien, Farben, Jahre, ...
- Relationen/Eigenschaften
  rot, rund, gerade, ungerade, prim, mehrstöckig, ...
  ist Bruder von, ist größer als, ist Teil von, hat Farbe, besitzt, ..
  $=$, $\geq$, ...
- Funktionen
  $+$, Mitte von, Vater von, Anfang von, ...

Beispiel 1

Objekte (Elemente): Zahlen

Funktionen: $+$, $*$

Terme: $2 + 3$, $3 * (5 + 6)$, x, $x + 2$, $x * (2 - y)$

Beispiel 1

Objekte (Elemente): Zahlen

Funktionen: $+$, $*$

Terme: $2+3$, $3*(5+6)$, x, $x+2$, $x*(2-y)$

Relationen: gerade, ungerade

Beispiel 1

Objekte (Elemente): Zahlen

Funktionen: $+$, $*$

Terme: $2+3, \quad 3*(5+6), \quad x, \quad x+2, \quad x*(2-y)$

Relationen: gerade, ungerade

Formel:

gerade(2), ungerade(5), gerade(100), ungerade(100)

gerade(2)$\wedge$ ungerade(5)

gerade(x) $\rightarrow$ gerade($x+1$)

Beispiel 1

Objekte (Elemente): Zahlen

Funktionen: $+$, $*$

Terme: $2+3$, $3*(5+6)$, x, $x+2$, $x*(2-y)$

Relationen/Eigenschaften: gerade, ungerade

Formel:

gerade(2), ungerade(5), gerade(100), ungerade(100)

gerade(2)$\wedge$ ungerade(5)

gerade(x) $\rightarrow$ gerade($x+1$)

Quantoren: $\forall$ (für alle); $\exists$ (es gibt)

Beispiel 1

Objekte (Elemente): Zahlen

Funktionen: $+$, $*$

Terme: $2+3, \quad 3*(5+6), \quad x, \quad x+2, \quad x*(2-y)$

Relationen/Eigenschaften: gerade, ungerade

Formel:

gerade(2), ungerade(5), gerade(100), ungerade(100)

gerade(2)$\wedge$ ungerade(5)

gerade(x) $\rightarrow$ gerade($x+1$)

Quantoren: $\forall$ (für alle); $\exists$ (es gibt)

Formeln mit Quantoren:

$\forall x$ gerade(x)$\vee$ gerade($x+1$)

$\exists x$ ungerade(x)

Beispiel 2:

- Objekte (Elemente): Menschen
- Funktionen: Vater, Mutter

Beispiel 2:

- Objekte (Elemente): Menschen
- Funktionen: Vater, Mutter, Jan, Anna

x	Jan	$Anna$
$Vater(x)$	$Vater(Jan)$	$Vater(Anna)$
$Mutter(x)$	$Mutter(Jan)$	$Mutter(Anna)$
$Vater(Mutter(x))$	$Vater(Mutter(Jan))$	...

Beispiel 2:

- Objekte (Elemente): Menschen
- Funktionen: Vater, Mutter, Jan, Anna

x	Jan	$Anna$
$Vater(x)$	$Vater(Jan)$	$Vater(Anna)$
$Mutter(x)$	$Mutter(Jan)$	$Mutter(Anna)$
$Vater(Mutter(x))$	$Vater(Mutter(Jan))$	...

- Eigenschaften: ist-Bruder-von; Mann; Frau

$Mann(x)$	$Mann(Jan)$	$Mann(Anna)$
$Mann(Vater(x))$	$Frau(Vater(Jan))$	$Mann(Vater(Jan))$
ist-Bruder-von(x, y)	ist-Bruder-von(x, Jan)	ist-Bruder-von$(x, Anna)$
		ist-Bruder-von$(Jan, Anna)$

Beispiel 2:

- Objekte (Elemente): Menschen
- Funktionen: Vater, Mutter, Jan, Anna

x	Jan	$Anna$
$Vater(x)$	$Vater(Jan)$	$Vater(Anna)$
$Mutter(x)$	$Mutter(Jan)$	$Mutter(Anna)$
$Vater(Mutter(x))$	$Vater(Mutter(Jan))$	...

- Eigenschaften: ist-Bruder-von; Mann; Frau

$Mann(x)$	$Mann(Jan)$	$Mann(Anna)$
$Mann(Vater(x))$	$Frau(Vater(Jan))$	$Mann(Vater(Jan))$
ist-Bruder-von(x, y)	ist-Bruder-von(x, Jan)	ist-Bruder-von$(x, Anna)$
		ist-Bruder-von$(Jan, Anna)$

Beispiel 2:

Formel:

$Mann(Vater(Jan))$

$Mann(Vater(Jan)) \wedge Frau(Mutter(Jan))$

$Mann(Mutter(Anna))$

$Mann(Vater(Jan)) \wedge$ ist-Bruder-von$(Jan, Anna)$

Beispiel 2:

Formel:

$Mann(Vater(Jan))$

$Mann(Vater(Jan)) \wedge Frau(Mutter(Jan))$

$Mann(Mutter(Anna))$

$Mann(Vater(Jan)) \wedge$ ist-Bruder-von$(Jan, Anna)$

Quantoren

$\forall$: für alle

$\exists$: es gibt

Formeln mit Quantoren:

$\forall x \quad Mann(Vater(x))$
$\forall x \quad Mann(Mutter(x))$
$\forall x, y$ (ist-Bruder-von$(x, y) \rightarrow Mann(x)$)

Beispiel 3

"Alle, die in Koblenz studieren, sind schlau"

- Objekte (Elemente): Menschen
- Funktionen: koblenz
- Eigenschaften: studiertIn, schlau

$\forall x(\text{studiertIn}(x, \textit{koblenz}) \rightarrow \text{schlau}(x))$

Beispiel 3

"Alle, die in Koblenz studieren, sind schlau"

- Objekte (Elemente): Menschen
- Funktionen: koblenz
- Eigenschaften: studiertIn, schlau

$\forall x(\text{studiertIn}(x, \mathit{koblenz}) \rightarrow \text{schlau}(x))$

"Es gibt jemand, der in Landau studiert und schlau ist"

- Objekte (Elemente): Menschen
- Funktionen: landau
- Eigenschaften: studiertIn, schlau

$\exists x(\text{studiertIn}(x, \mathit{landau}) \wedge \text{schlau}(x))$

Prädikatenlogik: Deduktionsmechanismus

- Deduktionsmechanismus

  Ableitung neuer wahrer Formeln

Syllogismen:

$$\frac{\forall x(P(x) \rightarrow Q(x)) \qquad \forall x(Q(x) \rightarrow R(x))}{\forall x(P(x) \rightarrow R(x))}$$

$$\frac{\forall x(\text{studiertIn}(x, \textit{koblenz}) \rightarrow \text{schlau}(x)) \quad \forall x(\text{schlau}(x) \rightarrow \text{gute-noten}(x))}{\forall x(\text{studiertIn}(x, \textit{koblenz}) \rightarrow \text{gute-noten}(x))}$$

Prädikatenlogik: Deduktionsmechanismus

- Deduktionsmechanismus

  Ableitung neuer wahrer Formeln

Syllogismen:

$$\frac{Q(a) \qquad \forall x(Q(x) \rightarrow R(x))}{R(a)}$$

Beispiel:

$$\frac{\text{studiertIn}(\mathit{Jan}, \mathit{koblenz}) \qquad \forall x(\text{studiertIn}(x, \mathit{koblenz}) \rightarrow \text{schlau}(x))}{\text{schlau}(\mathit{Jan})}$$

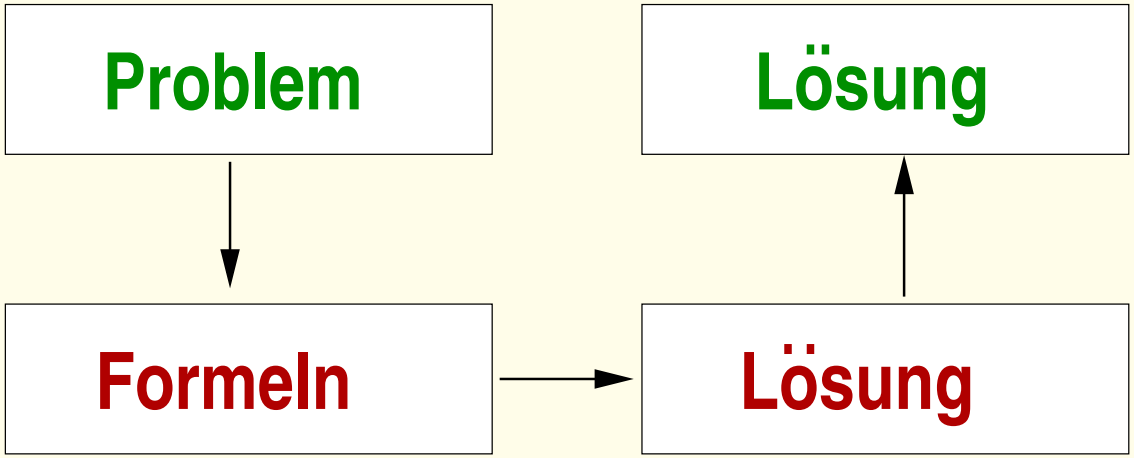
Prädikatenlogik: Deduktionsmechanismus

In dieser Vorlesung:

- Resolutionskalkül
- Tableaukalkül

Das Prinzip

z.B. natürliche Sprache



präzise Beschreibung

Anwendungesbeispiel: Sicherheitsprotokole

Ziel: zwei Personen (Alice und Bob) wollen miteinander kommunizieren

- über ein **unsicheres** Daten- oder Telefonnetz,
- **sicher**, d. h., ohne daß ein Eindringling (Charlie) mithören oder sich als Alice oder Bob ausgeben kann.

Beispiel: Sicherheitsprotokole

Ziel: zwei Personen (Alice und Bob) wollen miteinander kommunizieren

- über ein **unsicheres** Daten- oder Telefonnetz,
- **sicher**, d. h., ohne dass ein Eindringling (Charlie) mithören oder sich als Alice oder Bob ausgeben kann.

Hilfsmittel: Verschlüsselung

- Alice und Bob vereinbaren einen gemeinsamen Schlüssel und nutzen ihn, um ihr Gespräch zu verschlüsseln.
- Nur wer den Schlüssel kennt, kann das Gespräch entschlüsseln.

Beispiel: Sicherheitsprotokolle

Problem: wie kommen die Gesprächspartner an den gemeinsamen Schlüssel?

- Persönliche Übergabe kommt nicht immer in Frage.
- Wird der gemeinsame Schlüssel über das Netz unverschlüsselt verschickt, könnte Charlie ihn abfangen oder austauschen.
- Annahme: es gibt eine sichere Schlüsselzentrale, mit der Alice und Bob jeweils einen gemeinsamen Schlüssel vereinbart haben.

Beispiel: Sicherheitsprotokolle

Das folgende Schlüsselaustauschverfahren wurde 1993 von den beiden Kryptographen Neuman und Stubblebine vorgeschlagen:

Schritt 1:

Alice schickt (offen) Identifikation und Zufallszahl an Bob.

Beispiel: Sicherheitsprotokolle

Schritt 2:

Bob leitet Nachricht weiter an Schlüsselzentrale („Trust“).

Beispiel: Sicherheitsprotokolle

Schritt 3:

Trust schickt Nachricht an Alice. Darin: ein neuer gemeinsamer Schlüssel, einmal für Alice und einmal für Bob verschlüsselt.

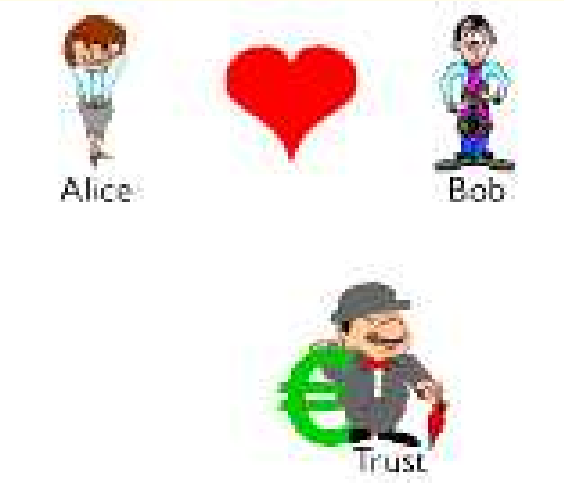
Beispiel: Sicherheitsprotokolle

Schritt 4:

Alice leitet den neuen gemeinsamen Schlüssel weiter an Bob.

Beispiel: Sicherheitsprotokolle

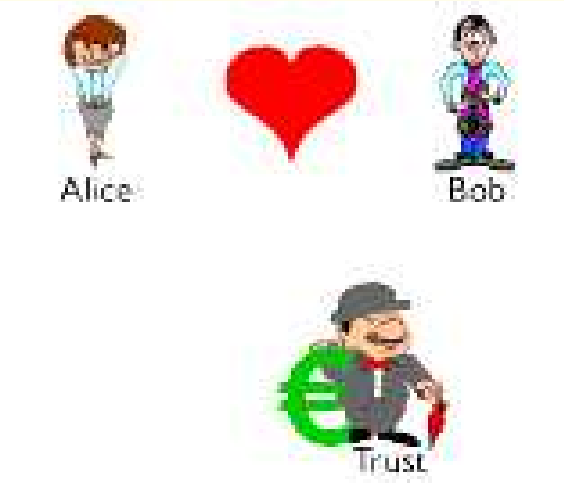
Schritt 5:



Alice und Bob können nun mit dem gemeinsamen Schlüssel kommunizieren.

Beispiel: Sicherheitsprotokolle

Ist das Verfahren sicher?



Wir übersetzen das Problem in Formeln und lassen sie von einem Theorembeweiser untersuchen.

Beispiel: Sicherheitsprotokolle

Zuerst formalisieren wir die Eigenschaften des Protokolls:

- Wenn Alice/Bob/Trust eine Nachricht in einem bestimmten Format bekommt, dann schickt er/sie eine andere Nachricht ab.

Beispiel: Sicherheitsprotokolle

Zuerst formalisieren wir die Eigenschaften des Protokolls:

- Wenn Alice/Bob/Trust eine Nachricht in einem bestimmten Format bekommt, dann schickt er/sie eine andere Nachricht ab.

Dann formalisieren wir die Eigenschaften des Angreifers:

- Wenn eine Nachricht übermittelt wird, kann Charlie sie mithören.
- Wenn Charlie eine verschlüsselte Nachricht bekommt und den passenden Schlüssel hat, kann er sie entschlüsseln.
- Wenn Charlie eine Nachricht hat, dann kann er sie an Alice/Bob/Trust abschicken.

  ...

Formalisierung

Zum Schluss müssen wir noch formalisieren was es bedeutet, dass der Angreifer Erfolg hat.

Dies ist dann der Fall, wenn er einen Schlüssel zur Kommunikation mit Bob hat, von dem Bob glaubt, es sei ein Schlüssel für Alice.

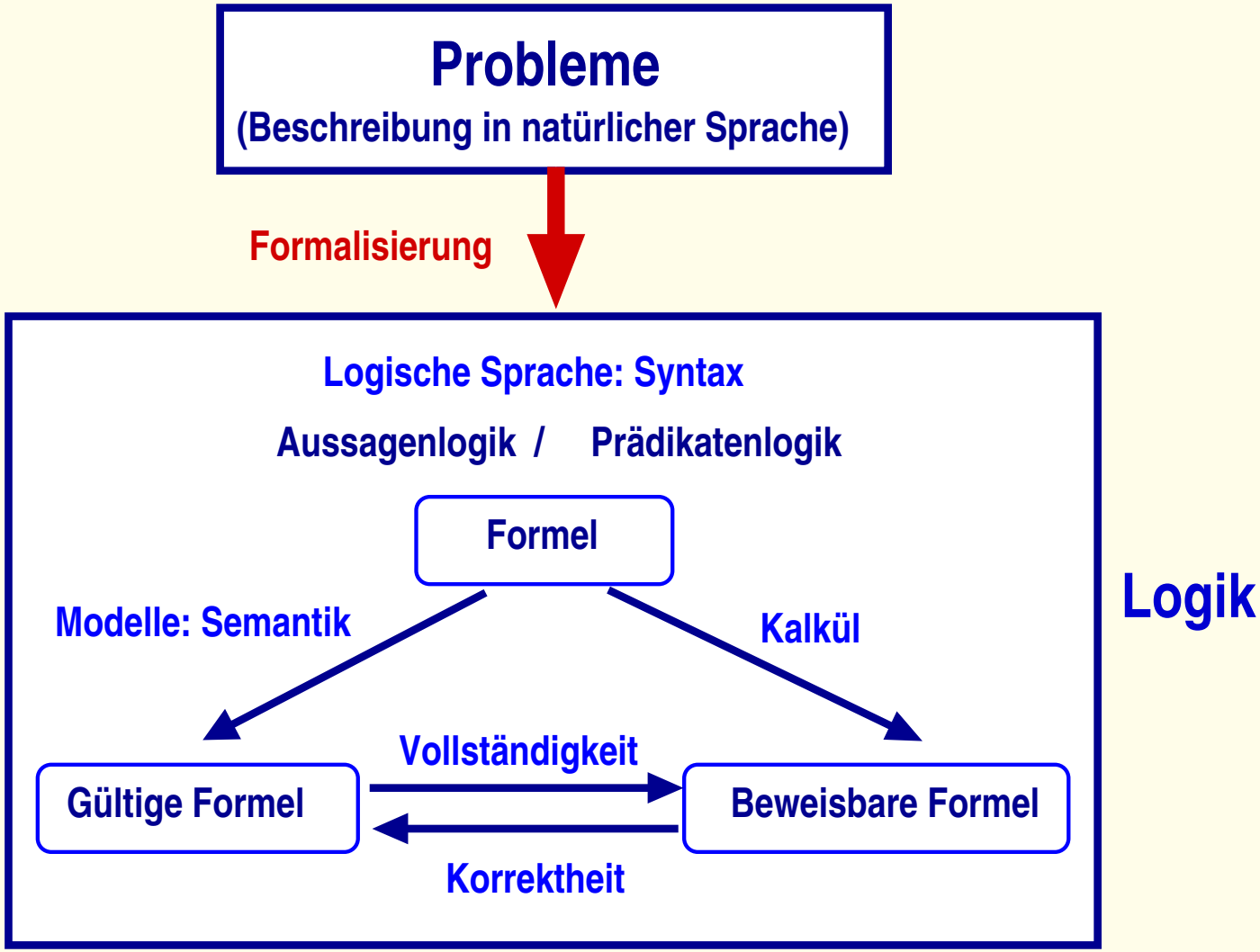
$\exists x[Ik(key(x, b)) \wedge Bk(key(x, a))]$

Automatische Analyse

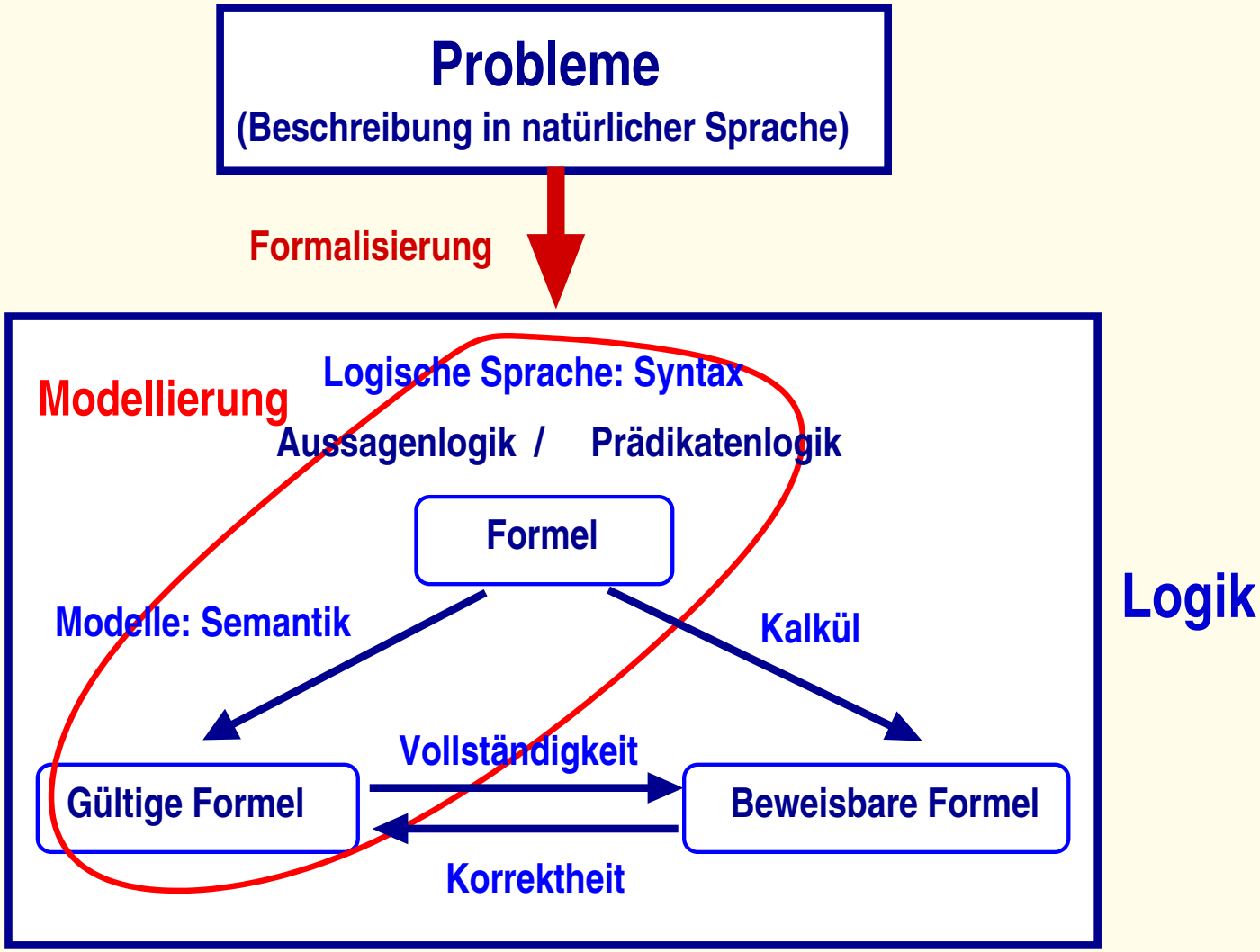
Die Formalisierung des Protokolls, Formeln (1)-(8) zusammen mit den Angreiferformeln (9)-(20) und der Erfolgsbedingung für den Angreifer kann man nun in einen Theorembeweiser eingeben.

Der Theorembeweiser beweist dann automatisch, dass der Angreifer das Protokoll brechen kann.

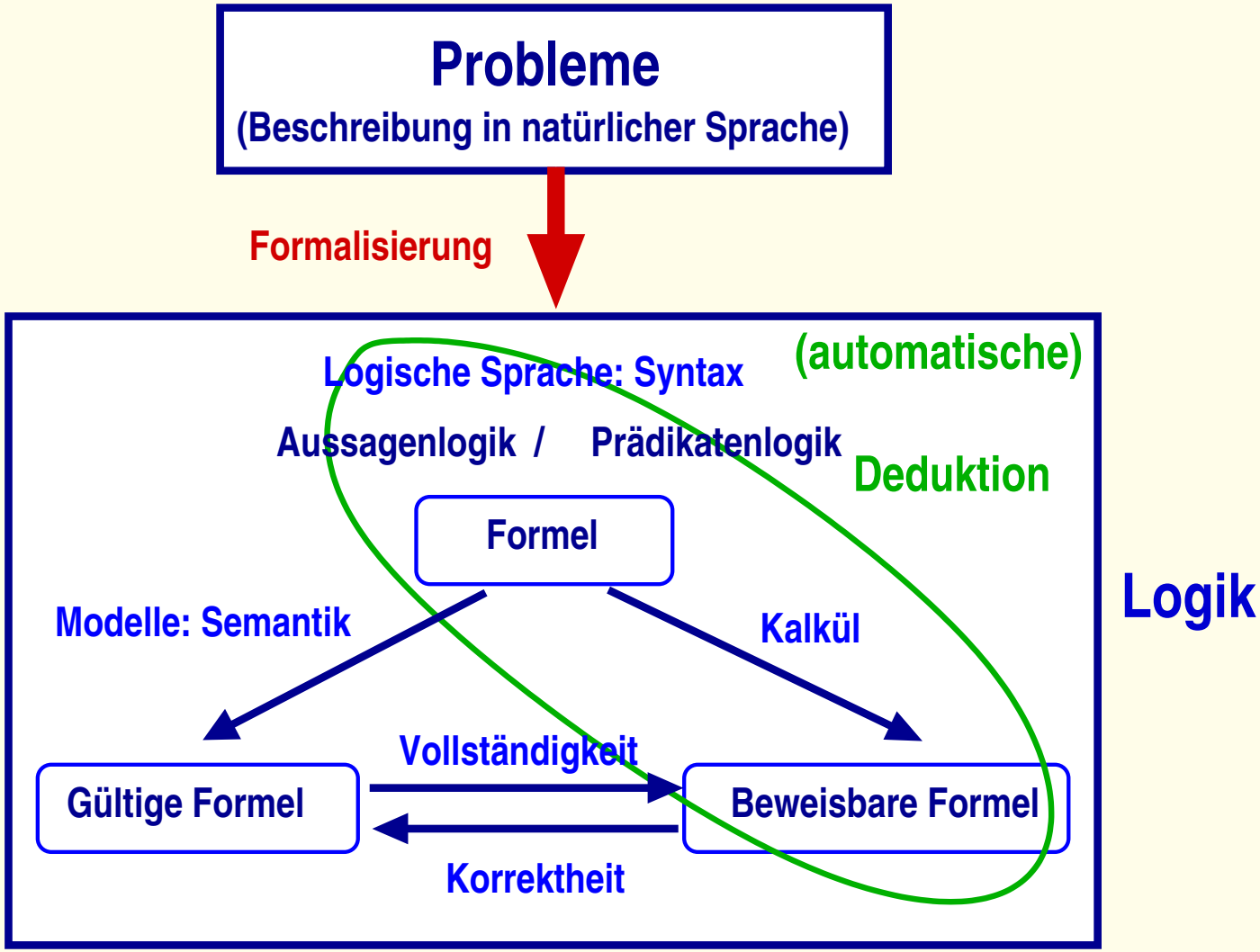
Das ganze Bild



Das ganze Bild



Das ganze Bild



Inhalt der Vorlesung

- **1. Einführung:** Motivation, Beweisstrategien (insb. Induktion)

Inhalt der Vorlesung

- **1. Einführung:** Motivation, Beweisstrategien (insb. Induktion)
- **2. Aussagenlogik**
  - Syntax und Semantik
  - Deduktionsmechanismen:
    - Resolution, Vollständigkeits- und Korrektheitsbeweise
    - Analytische Tableaux

Inhalt der Vorlesung

- **1. Einführung:** Motivation, Beweisstrategien (insb. Induktion)
- **2. Aussagenlogik**
  - Syntax und Semantik
  - Deduktionsmechanismen:
    - Resolution, Vollständigkeits- und Korrektheitsbeweise
    - Analytische Tableaux
- **3. Prädikatenlogik**
  - Syntax und Semantik
  - Deduktionsmechanismen:
    - Resolution, Vollständigkeits- und Korrektheitsbeweise
    - Analytische Tableaux

Inhalt der Vorlesung

- **1. Einführung:** Motivation, Beweisstrategien (insb. Induktion)
- **2. Aussagenlogik**
  - Syntax und Semantik
  - Deduktionsmechanismen:
    - Resolution, Vollständigkeits- und Korrektheitsbeweise
    - Analytische Tableaux
- **3. Prädikatenlogik**
  - Syntax und Semantik
  - Deduktionsmechanismen:
    - Resolution, Vollständigkeits- und Korrektheitsbeweise
    - Analytische Tableaux
- **4. Weitere Aussichten**

  - Nichtklassische Logiken; Logiken höherer Stufe
  - Anwendungen: z.B. Datenbanken oder Verifikation

Einführung: Zusammenfassung

- Ziel und Rolle der Formalen Logik in der Informatik
- Modellierung, Adäquatheit der Modellierung
- Wesentliche Komponenten für jede Logik: Syntax, Semantik, Deduktionsmechanismus (Kalkül)
- Beispiel Aussagenlogik: Syntax, Semantik, Syllogismen
- Beispiel Prädikatenlogik: Syntax, Semantik, Syllogismen
- The Whole Picture:
  - Formel in der "wahren Welt" / (semantisch) gültige Formel, gültige Formel / ableitbare Formel
  - Vollständigkeit und Korrektheit von Kalkülen