



Einführung in die Theoretische Informatik

David Drexel

Alexander Maringele

Julian Fodor

David Obwaller

Alexander Lochmann

Jonas Schöpf

Georg Moser

cbr.uibk.ac.at



Zusammenfassung

Zusammenfassung der letzten LVA

Definition

Die **Formeln** der Aussagenlogik sind induktiv definiert:

- 1 Eine atomare Formel p ist eine **Formel**,
- 2 ein Wahrheitswertsymbol (True, False) ist eine **Formel**, und
- 3 wenn A und B **Formeln** sind, dann sind

$$\neg A \quad (A \wedge B) \quad (A \vee B) \quad (A \rightarrow B)$$

auch **Formeln**

Definitionen

- Erweiterung der Belegung v zu einem **Wahrheitswert** \bar{v} für Formeln
- $A \equiv B$, wenn $A \models B$ und $B \models A$ gilt

Beispiel (Kontraposition in der Realität)

We arrive at the following paradox in a globalised world: when nationalists pursue more formal sovereignty they achieve less real sovereignty of the people. They want to take back control and they end up with less control. That's what the UK will end up with. And that's also what the Catalan nationalists will achieve if they pursue their nationalistic dreams.

Yet this paradox also has a corollary: when countries in Europe renounce formal sovereignty this leads to more real sovereignty for the peoples of Europe.¹

¹Paul De Grauwe, <https://blogs.lse.ac.uk/brexit/2017/10/06/the-catalan-crisis-and-brexit-stem-from-the-same-kind-of-nationalism/>

Beispiel (Kontraposition in der Realität)

We arrive at the following paradox in a globalised world: when nationalists pursue more formal sovereignty they achieve less real sovereignty of the people. They want to take back control and they end up with less control. That's what the UK will end up with. And that's also what the Catalan nationalists will achieve if they pursue their nationalistic dreams.

*Yet this paradox also has a **corollary**: when countries in Europe renounce formal sovereignty this leads to more real sovereignty for the peoples of Europe.¹*

¹Paul De Grauwe, <https://blogs.lse.ac.uk/brexit/2017/10/06/the-catalan-crisis-and-brexit-stem-from-the-same-kind-of-nationalism/>

Beispiel (Kontraposition in der Realität)

We arrive at the following paradox in a globalised world: when nationalists pursue more formal sovereignty they achieve less real sovereignty of the people. They want to take back control and they end up with less control. That's what the UK will end up with. And that's also what the Catalan nationalists will achieve if they pursue their nationalistic dreams.

Yet this paradox also has a corollary: when countries in Europe renounce formal sovereignty this leads to more real sovereignty for the peoples of Europe.¹

Beispiel

Formal stellt sich das „Korollar“ wie folgt dar:

$$\begin{aligned} & \text{„more formal sovereignty“} \rightarrow \text{„less real sovereignty“} \models \\ & \models \neg \text{„more formal sovereignty“} \rightarrow \neg \text{„less real sovereignty“} \end{aligned}$$

¹Paul De Grauwe, <https://blogs.lse.ac.uk/brexit/2017/10/06/the-catalan-crisis-and-brexit-stem-from-the-same-kind-of-nationalism/>

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, **Formales Beweisen, Konjunktive und Disjunktive Normalformen**

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

1 *A ist eine Tautologie gdw.*

$A\{p \mapsto \text{True}\}$ ist Tautologie und $A\{p \mapsto \text{False}\}$ ist Tautologie

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

1 *A ist eine Tautologie gdw.*

$A\{p \mapsto \text{True}\}$ ist Tautologie und $A\{p \mapsto \text{False}\}$ ist Tautologie

2 *A ist unerfüllbar gdw.*

$A\{p \mapsto \text{True}\}$ unerfüllbar und $A\{p \mapsto \text{False}\}$ unerfüllbar

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

1 *A ist eine Tautologie gdw.*

$A\{p \mapsto \text{True}\}$ ist Tautologie und $A\{p \mapsto \text{False}\}$ ist Tautologie

2 *A ist unerfüllbar gdw.*

$A\{p \mapsto \text{True}\}$ unerfüllbar und $A\{p \mapsto \text{False}\}$ unerfüllbar

Beispiel (Wahrheitstabellen oder logische Äquivalenzen)

Wir betrachten die Formel F

$$F := [(p \wedge q \rightarrow r) \wedge (p \rightarrow q)] \rightarrow (p \rightarrow r)$$

Es ist nicht schwer einzusehen, dass F eine Tautologie ist

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

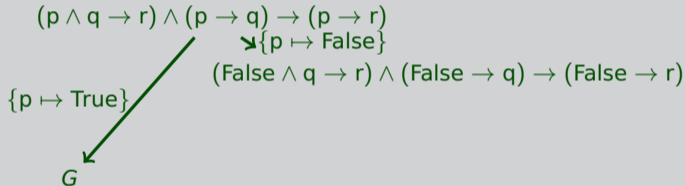
- 1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie
- 2 $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$ ist Tautologie

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

- 1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie
- 2 $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$ ist Tautologie

Anforderungen in Baumform:



Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

- 1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie
- 2 $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$ ist Tautologie

Anforderungen in Baumform:

$$\begin{array}{l} (p \wedge q \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r) \\ \quad \searrow \{p \mapsto \text{False}\} \\ \quad \quad \quad (\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r) \\ \quad \quad \quad \equiv \\ \quad \quad \quad (\text{False} \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow \text{True} \end{array}$$

$\{p \mapsto \text{True}\}$ \swarrow G

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

- 1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie
- 2 $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$ ist Tautologie

Anforderungen in Baumform:

$$\begin{array}{l} (p \wedge q \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r) \\ \quad \searrow \{p \mapsto \text{False}\} \\ \quad \quad \quad (\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r) \\ \quad \quad \quad \equiv \\ \quad \quad \quad (\text{False} \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow \text{True} \\ \quad \quad \quad \equiv \\ \quad \quad \quad \text{True} \wedge \text{True} \rightarrow \text{True} \\ \quad \quad \quad \equiv \\ \quad \quad \quad \text{True} \end{array}$$

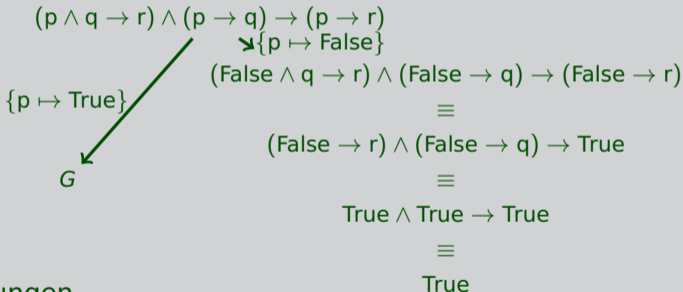
$\{p \mapsto \text{True}\}$ \swarrow G

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

- 1 $(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r) =: G$ ist Tautologie
- 2 $(\text{False} \wedge q \rightarrow r) \wedge (\text{False} \rightarrow q) \rightarrow (\text{False} \rightarrow r)$ ist Tautologie

Anforderungen in Baumform:




Übrige Anforderungen

- 3 G ist Tautologie

Beispiel (Fortsetzung)

$$\overbrace{(\text{True} \wedge q \rightarrow r) \wedge (\text{True} \rightarrow q) \rightarrow (\text{True} \rightarrow r)}^G$$

$$\{q \mapsto \text{True}\}$$


$$\{q \mapsto \text{False}\}$$


Beispiel (Fortsetzung)

$$\begin{array}{c} \overbrace{(True \wedge q \rightarrow r) \wedge (True \rightarrow q) \rightarrow (True \rightarrow r)}^G \\ \equiv \\ (q \rightarrow r) \wedge q \rightarrow r \\ \swarrow \quad \searrow \\ \{q \mapsto True\} \quad \{q \mapsto False\} \end{array}$$

Beispiel (Fortsetzung)

$$\begin{array}{c} \overbrace{(True \wedge q \rightarrow r) \wedge (True \rightarrow q) \rightarrow (True \rightarrow r)}^G \\ \equiv \\ (q \rightarrow r) \wedge q \rightarrow r \\ \swarrow \quad \searrow \\ \begin{array}{l} \{q \mapsto True\} \\ (True \rightarrow r) \wedge True \rightarrow r \end{array} \quad \begin{array}{l} \{q \mapsto False\} \\ (False \rightarrow r) \wedge False \rightarrow r \end{array} \end{array}$$

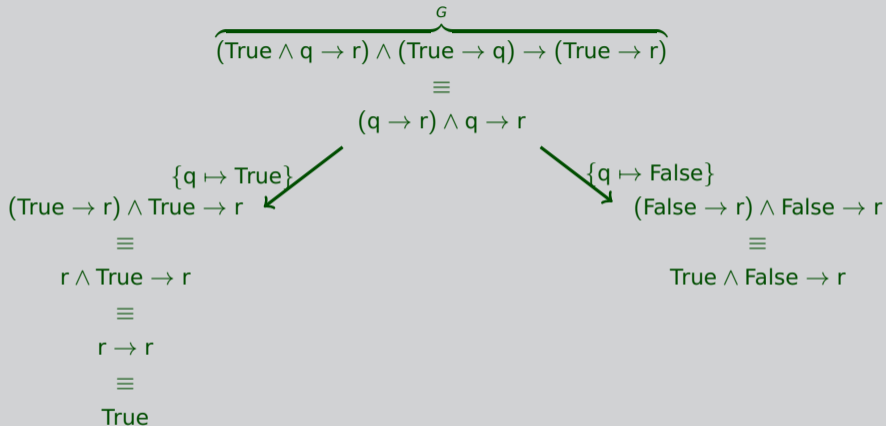
Beispiel (Fortsetzung)

$$\begin{array}{c} \overbrace{(True \wedge q \rightarrow r) \wedge (True \rightarrow q) \rightarrow (True \rightarrow r)}^G \\ \equiv \\ (q \rightarrow r) \wedge q \rightarrow r \\ \swarrow \{q \mapsto True\} \quad \searrow \{q \mapsto False\} \\ (True \rightarrow r) \wedge True \rightarrow r \quad (False \rightarrow r) \wedge False \rightarrow r \\ \equiv \\ r \wedge True \rightarrow r \end{array}$$

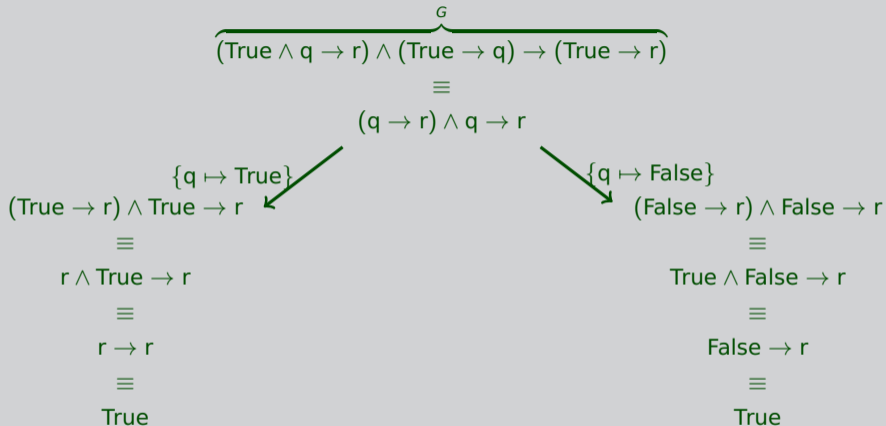
Beispiel (Fortsetzung)

$$\begin{array}{c} \overbrace{(True \wedge q \rightarrow r) \wedge (True \rightarrow q) \rightarrow (True \rightarrow r)}^G \\ \equiv \\ (q \rightarrow r) \wedge q \rightarrow r \\ \swarrow \{q \mapsto True\} \quad \searrow \{q \mapsto False\} \\ (True \rightarrow r) \wedge True \rightarrow r \quad (False \rightarrow r) \wedge False \rightarrow r \\ \equiv \\ r \wedge True \rightarrow r \\ \equiv \\ r \rightarrow r \\ \equiv \\ True \end{array}$$

Beispiel (Fortsetzung)



Beispiel (Fortsetzung)



Beispiel (Fortsetzung)

$$\begin{array}{c} \overbrace{(True \wedge q \rightarrow r) \wedge (True \rightarrow q) \rightarrow (True \rightarrow r)}^G \\ \equiv \\ (q \rightarrow r) \wedge q \rightarrow r \\ \swarrow \{q \mapsto True\} \quad \searrow \{q \mapsto False\} \\ \begin{array}{c} (True \rightarrow r) \wedge True \rightarrow r \\ \equiv \\ r \wedge True \rightarrow r \\ \equiv \\ r \rightarrow r \\ \equiv \\ True \end{array} \\ \quad \quad \quad \begin{array}{c} (False \rightarrow r) \wedge False \rightarrow r \\ \equiv \\ True \wedge False \rightarrow r \\ \equiv \\ False \rightarrow r \\ \equiv \\ True \end{array} \end{array}$$

Es gibt keine weiteren Anforderungen mehr, also ist F eine Tautologie

Modus Ponens

$$\frac{A \rightarrow B \quad A}{B} \text{ MP}$$

Modus Ponens

$$\frac{A \rightarrow B \quad A}{B} \text{ MP}$$

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- (1) $A \rightarrow (B \rightarrow A)$
- (2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- (3) $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

Formales Beweisen

Modus Ponens

$$\frac{A \rightarrow B \quad A}{B} \text{ MP}$$

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- (1) $A \rightarrow (B \rightarrow A)$
- (2) $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- (3) $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

Die Axiome sind Schemata, das heißt A , B und C können für beliebige Formeln stehen

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

- $A_i \in \mathcal{G}$

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

- $A_i \in \mathcal{G}$
- A_i ist eines der Axiome

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

- $A_i \in \mathcal{G}$
- A_i ist eines der Axiome
- A_i folgt mit MP aus A_{i_1} und A_{i_2} , $i_1, i_2 < i$

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

- $A_i \in \mathcal{G}$
- A_i ist eines der Axiome
- A_i folgt mit MP aus A_{i_1} und A_{i_2} , $i_1, i_2 < i$

2 F heißt **beweisbar** aus den Annahmen \mathcal{G} , wenn es einen Beweis von F aus \mathcal{G} gibt

Definition

\mathcal{G} eine endliche Menge von Formeln, F eine Formel

1 Ein **Beweis** von F aus \mathcal{G} ist eine Sequenz

$$A_1, \dots, A_n = F$$

sodass für alle $1 \leq i \leq n$:

- $A_i \in \mathcal{G}$
- A_i ist eines der Axiome
- A_i folgt mit MP aus A_{i_1} und A_{i_2} , $i_1, i_2 < i$

2 F heißt **beweisbar** aus den Annahmen \mathcal{G} , wenn es einen Beweis von F aus \mathcal{G} gibt

Definition

1 Die **Beweisbarkeitsrelation** $A_1, \dots, A_n \vdash B$ gilt, gdw. B aus A_1, \dots, A_n beweisbar ist

2 Wir schreiben $\vdash A$ statt $\emptyset \vdash A$ und nennen A in diesem Fall **beweisbar**

Korrektheit und Vollständigkeit

Satz

Das Axiomensystem mit Inferenzregel MP ist *korrekt* und *vollständig* für die Aussagenlogik:

$$A_1, \dots, A_n \models B \quad \text{gdw.} \quad A_1, \dots, A_n \vdash B .$$

Korrektheit und Vollständigkeit

Satz

Das Axiomensystem mit Inferenzregel MP ist **korrekt** und **vollständig** für die Aussagenlogik:

$$A_1, \dots, A_n \models B \quad \text{gdw.} \quad A_1, \dots, A_n \vdash B .$$

Fakt

Basierend auf einem korrekten und vollständigen Beweissystem können wir versuchen das Beweisen zu automatisieren → **SAT solvers**

Korrektheit und Vollständigkeit

Satz

Das Axiomensystem mit Inferenzregel MP ist **korrekt** und **vollständig** für die Aussagenlogik:

$$A_1, \dots, A_n \models B \quad \text{gdw.} \quad A_1, \dots, A_n \vdash B.$$

Fakt

Basierend auf einem korrekten und vollständigen Beweissystem können wir versuchen das Beweisen zu automatisieren → **SAT solvers**

Satz (Deduktionstheorem)

Sei B mit Hilfe der Prämisse A beweisbar, dann existiert ein Beweis von $A \rightarrow B$, der A nicht als Prämisse hat

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

p	q	$\neg p \rightarrow (p \rightarrow q)$	p	q	$\neg p \rightarrow (p \rightarrow q)$
T	T	T	F	T	T
T	F	T	F	F	T

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

$$6 \quad \neg p \rightarrow (p \rightarrow q)$$

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1

$\neg p$

Prämisse

2

3

4

5

6

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

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3		
4		
5		
6	$\neg p \rightarrow (p \rightarrow q)$	

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, <i>Modus Ponens</i>
4		
5		
6	$\neg p \rightarrow (p \rightarrow q)$	

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, <i>Modus Ponens</i>
4	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Axiom (3)
5		
6	$\neg p \rightarrow (p \rightarrow q)$	

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, <i>Modus Ponens</i>
4	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Axiom (3)
5	$p \rightarrow q$	3, 4, <i>Modus Ponens</i>
6	$\neg p \rightarrow (p \rightarrow q)$	

Beispiel

Wir betrachten die Tautologie $\neg p \rightarrow (p \rightarrow q)$:

$$(1) \quad A \rightarrow (B \rightarrow A)$$

$$(2) \quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$$

$$(3) \quad (\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$$

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \rightarrow (\neg q \rightarrow \neg p)$	Axiom (1)
3	$\neg q \rightarrow \neg p$	1, 2, <i>Modus Ponens</i>
4	$(\neg q \rightarrow \neg p) \rightarrow (p \rightarrow q)$	Axiom (3)
5	$p \rightarrow q$	3, 4, <i>Modus Ponens</i>
6	$\neg p \rightarrow (p \rightarrow q)$	1, 5, <i>Deduktionstheorem</i>

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen;

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$;

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

1 Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \rightarrow A$ beweisbar

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

1 Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \rightarrow A$ beweisbar

2 Schritt: $k > 1$; die Induktionshypothese besagt

Für alle $l < k$ ist $A \rightarrow B_l$ ohne die Prämisse A beweisbar

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

1 Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \rightarrow A$ beweisbar

2 Schritt: $k > 1$; die Induktionshypothese besagt

Für alle $l < k$ ist $A \rightarrow B_l$ ohne die Prämisse A beweisbar

Fallunterscheidung:

- sei $B_k = A$ (wir argumentieren wie im Basisfall)

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

1 Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \rightarrow A$ beweisbar

2 Schritt: $k > 1$; die Induktionshypothese besagt

Für alle $l < k$ ist $A \rightarrow B_l$ ohne die Prämisse A beweisbar

Fallunterscheidung:

- sei $B_k = A$ (wir argumentieren wie im Basisfall)
- sei B_k ein Axiom oder eine Prämisse $\neq A$

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

$$B_1, \dots, B_\ell = B$$

nachgewiesen; oBdA. gilt $B_1 = A$; wir zeigen die folgende Aussage mit Induktion nach k ($1 \leq k \leq \ell$):

$A \rightarrow B_k$ ist ohne die Prämisse A beweisbar

1 Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \rightarrow A$ beweisbar

2 Schritt: $k > 1$; die Induktionshypothese besagt

Für alle $l < k$ ist $A \rightarrow B_l$ ohne die Prämisse A beweisbar

Fallunterscheidung:

- sei $B_k = A$ (wir argumentieren wie im Basisfall)
- sei B_k ein Axiom oder eine Prämisse $\neq A$
- B_k folgt mit MP aus $B_i, B_j = (B_i \rightarrow B_k)$

Beweis des Deduktionstheorems.

- Fall B_k ein Axiom oder eine Prämisse $\neq A$

Beweis des Deduktionstheorems.

- Fall B_k ein Axiom oder eine Prämisse $\neq A$

- Fall B_k folgt mit MP aus $B_i, B_j = (B_i \rightarrow B_k)$

Beweis des Deduktionstheorems.

- Fall B_k ein Axiom oder eine Prämisse $\neq A$

Wir verwenden folgenden Beweis:

- 1 B_k Axiom oder Prämisse $\neq A$
- 2 $B_k \rightarrow (A \rightarrow B_k)$ Axiom (1)
- 3 $A \rightarrow B_k$ 1, 2, MP

- Fall B_k folgt mit MP aus $B_i, B_j = (B_i \rightarrow B_k)$

Beweis des Deduktionstheorems.

- Fall B_k ein Axiom oder eine Prämisse $\neq A$

Wir verwenden folgenden Beweis:

- 1 B_k Axiom oder Prämisse $\neq A$
- 2 $B_k \rightarrow (A \rightarrow B_k)$ Axiom (1)
- 3 $A \rightarrow B_k$ 1, 2, MP

- Fall B_k folgt mit MP aus $B_i, B_j = (B_i \rightarrow B_k)$

Wir verwenden folgenden Beweis:

- 1 Beweis von $A \rightarrow B_i$ IH
- 2 Beweis von $A \rightarrow (B_i \rightarrow B_k)$ IH
- 3 $(A \rightarrow (B_i \rightarrow B_k)) \rightarrow (A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$ Axiom (2)
- 4 $(A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$ 2, 3, MP
- 5 $A \rightarrow B_k$ 1, 4, MP

Beweis des Deduktionstheorems.

- Fall B_k ein Axiom oder eine Prämisse $\neq A$

Wir verwenden folgenden Beweis:

- 1 B_k Axiom oder Prämisse $\neq A$
- 2 $B_k \rightarrow (A \rightarrow B_k)$ Axiom (1)
- 3 $A \rightarrow B_k$ 1, 2, MP

- Fall B_k folgt mit MP aus $B_i, B_j = (B_i \rightarrow B_k)$

Wir verwenden folgenden Beweis:

- 1 Beweis von $A \rightarrow B_i$ IH
- 2 Beweis von $A \rightarrow (B_i \rightarrow B_k)$ IH
- 3 $(A \rightarrow (B_i \rightarrow B_k)) \rightarrow (A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$ Axiom (2)
- 4 $(A \rightarrow B_i) \rightarrow (A \rightarrow B_k)$ 2, 3, MP
- 5 $A \rightarrow B_k$ 1, 4, MP

Definition

Eine **Wahrheitsfunktion** $f: \{T, F\}^n \rightarrow \{T, F\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

Eine **Wahrheitsfunktion** $f: \{T, F\}^n \rightarrow \{T, F\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

Sei $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion; wir definieren:

$$\mathbf{TV}(f) := \{(s_1, \dots, s_n) \mid f(s_1, \dots, s_n) = T\}$$

Definition

Eine **Wahrheitsfunktion** $f: \{T, F\}^n \rightarrow \{T, F\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

Sei $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion; wir definieren:

$$\text{TV}(f) := \{(s_1, \dots, s_n) \mid f(s_1, \dots, s_n) = T\}$$

Definition (Konjunktive und Disjunktive Normalform)

- 1 Ein **Literal** ist ein Atom p oder die Negation eines Atoms $\neg p$

Definition

Eine **Wahrheitsfunktion** $f: \{T, F\}^n \rightarrow \{T, F\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

Sei $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion; wir definieren:

$$\text{TV}(f) := \{(s_1, \dots, s_n) \mid f(s_1, \dots, s_n) = T\}$$

Definition (Konjunktive und Disjunktive Normalform)

- 1 Ein **Literal** ist ein Atom p oder die Negation eines Atoms $\neg p$
- 2 Formel A ist in **disjunktiver Normalform (DNF)**, wenn A eine Disjunktion von Konjunktionen von Literalen

Definition

Eine **Wahrheitsfunktion** $f: \{T, F\}^n \rightarrow \{T, F\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

Sei $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion; wir definieren:

$$\text{TV}(f) := \{(s_1, \dots, s_n) \mid f(s_1, \dots, s_n) = T\}$$

Definition (Konjunktive und Disjunktive Normalform)

- 1 Ein **Literal** ist ein Atom p oder die Negation eines Atoms $\neg p$
- 2 Formel A ist in **disjunktiver Normalform (DNF)**, wenn A eine Disjunktion von Konjunktionen von Literalen
- 3 Formel A ist in **konjunktiver Normalform (KNF)**, wenn A eine Konjunktion von Disjunktionen von Literalen

- $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion
 $TV(f) \neq \emptyset, TV(f) \neq \{T, F\}^n$

Lemma

- $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion
 $TV(f) \neq \emptyset, TV(f) \neq \{T, F\}^n$
- p_1, \dots, p_n atomare Formeln

Lemma

- $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion
 $TV(f) \neq \emptyset, TV(f) \neq \{T, F\}^n$
- p_1, \dots, p_n atomare Formeln
- Sei DNF D definiert als:

$$D := \bigvee_{(s_1, \dots, s_n) \in TV(f)} \bigwedge_{i=1}^n A_i$$

wobei $A_i = p_i$, wenn $s_i = T$ und $A_i = \neg p_i$ sonst

Lemma

- $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion
 $\text{TV}(f) \neq \emptyset, \text{TV}(f) \neq \{T, F\}^n$
- p_1, \dots, p_n atomare Formeln
- Sei DNF D definiert als:

$$D := \bigvee_{(s_1, \dots, s_n) \in \text{TV}(f)} \bigwedge_{i=1}^n A_i$$

wobei $A_i = p_i$, wenn $s_i = T$ und $A_i = \neg p_i$ sonst

- Sei KNF K definiert als:

$$K := \bigwedge_{(s_1, \dots, s_n) \notin \text{TV}(f)} \bigvee_{j=1}^n B_j$$

wobei $B_j = \neg p_j$, wenn $s_j = T$ und $B_j = p_j$ sonst

Lemma

- $f: \{T, F\}^n \rightarrow \{T, F\}$ eine Wahrheitsfunktion
 $\text{TV}(f) \neq \emptyset, \text{TV}(f) \neq \{T, F\}^n$
- p_1, \dots, p_n atomare Formeln
- Sei DNF D definiert als:

$$D := \bigvee_{(s_1, \dots, s_n) \in \text{TV}(f)} \bigwedge_{i=1}^n A_i$$

wobei $A_i = p_i$, wenn $s_i = T$ und $A_i = \neg p_i$ sonst

- Sei KNF K definiert als:

$$K := \bigwedge_{(s_1, \dots, s_n) \notin \text{TV}(f)} \bigvee_{j=1}^n B_j$$

wobei $B_j = \neg p_j$, wenn $s_j = T$ und $B_j = p_j$ sonst

- Die Wahrheitstabellen von D und K entsprechen der Wahrheitsfunktion f

1 *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*

- 1 *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
- 2 *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Satz

- 1 *Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden*
- 2 *Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen*

Beweis.

- 1 Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
 - $TV(f) = \emptyset$
 - $TV(f) = \{T, F\}^n$

Satz

- 1 Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden
- 2 Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen

Beweis.

- 1 Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
 - $TV(f) = \emptyset$
 - $TV(f) = \{T, F\}^n$
- 2 Setze $D = K := \bigwedge_{i=1}^n (p_i \wedge \neg p_i)$ im ersten Fall
- 3 Setze $D = K := \bigvee_{i=1}^n (p_i \vee \neg p_i)$ im zweiten Fall

Satz

- 1 Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden
- 2 Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen

Beweis.

- 1 Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:

- $TV(f) = \emptyset$
- $TV(f) = \{T, F\}^n$

- 2 Setze $D = K := \bigwedge_{i=1}^n (p_i \wedge \neg p_i)$ im ersten Fall

- 3 Setze $D = K := \bigvee_{i=1}^n (p_i \vee \neg p_i)$ im zweiten Fall

Satz

- 1 Jede Wahrheitsfunktion kann als DNF oder KNF ausgedrückt werden
- 2 Jede Formel mit n Atomen induziert eine Wahrheitsfunktion in n Variablen

Beweis.

- 1 Es fehlen die Fälle, wo die Wahrheitsfunktion trivial ist:
 - $\text{TV}(f) = \emptyset$
 - $\text{TV}(f) = \{\text{T}, \text{F}\}^n$
- 2 Setze $D = K := \bigwedge_{i=1}^n (p_i \wedge \neg p_i)$ im ersten Fall
- 3 Setze $D = K := \bigvee_{i=1}^n (p_i \vee \neg p_i)$ im zweiten Fall

Folgerung

Für jede Formel A existiert eine DNF D und eine KNF K , sodass $A \equiv D \equiv K$ gilt.

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F, T), (T, F)\}$$

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F, T), (T, F)\}$$

p ₁	p ₂	$p_1 \oplus p_2$	Disjunktion
F	F	F	
F	T	T	
T	F	T	
T	T	F	

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F, T), (T, F)\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion
F	F	F	$p_1 \vee p_2$
T	T	F	

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F, T), (T, F)\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion
F	F	F	$p_1 \vee p_2$
T	T	F	$\neg p_1 \vee \neg p_2$

Beispiel

Die folgende Operation (\oplus) wird XOR genannt:

p	q	$p \oplus q$
F	F	F
F	T	T
T	F	T
T	T	F

Wir erstellen die KNF.

$$TV(\oplus) = \{(F, T), (T, F)\}$$

p_1	p_2	$p_1 \oplus p_2$	Disjunktion	KNF
F	F	F	$p_1 \vee p_2$	
T	T	F	$\neg p_1 \vee \neg p_2$	$(p_1 \vee p_2) \wedge (\neg p_1 \vee \neg p_2)$