

Einführung in die Theoretische Informatik

Christian Dalvit Manuel Eberl

Samuel Frontull **Cezary Kaliszyk** Daniel Ranalter

Wintersemester 2022/23

Zusammenfassung

Wintersemester 2022/23

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

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Kalkül des natürlichen Schließens, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

algebraische Strukturen, Boolesche Algebra

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen, Chomsky-Hierarchie, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Kalkül des natürlichen Schließens, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

algebraische Strukturen, Boolesche Algebra

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen, Chomsky-Hierarchie, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Methode von Quine

Wintersemester 2022/23

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

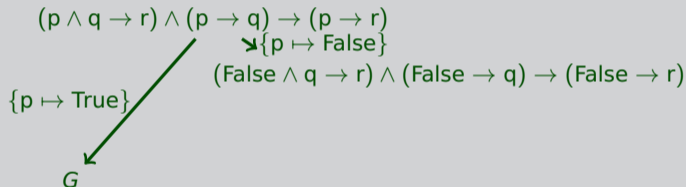
Beispiel (Methode von Quine)

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:

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

$\{p \mapsto \text{True}\}$ \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:

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


Übrige Anforderungen

3 G ist Tautologie

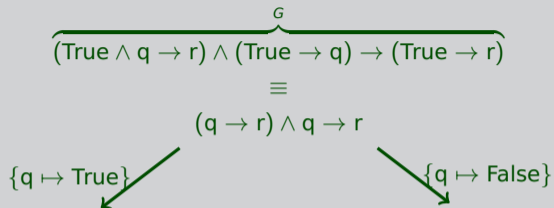
Beispiel (Fortsetzung)

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

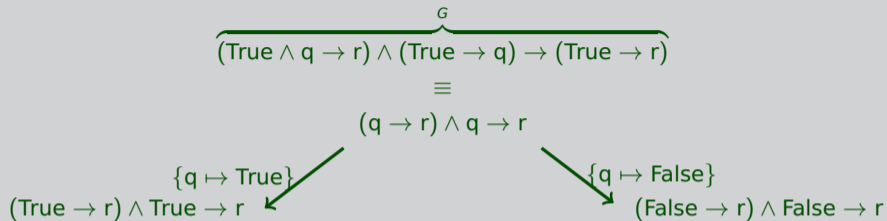
$$\{q \mapsto \text{True}\}$$


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


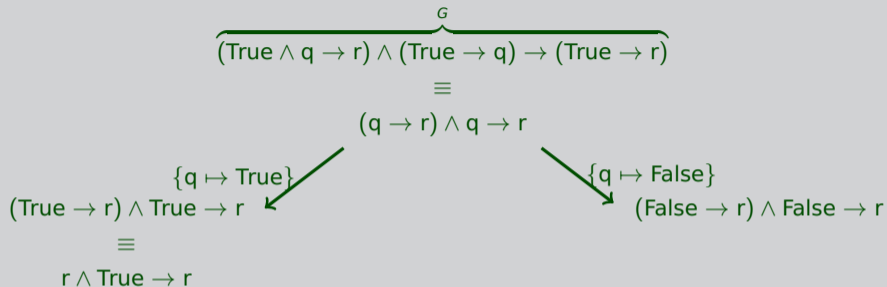
Beispiel (Fortsetzung)



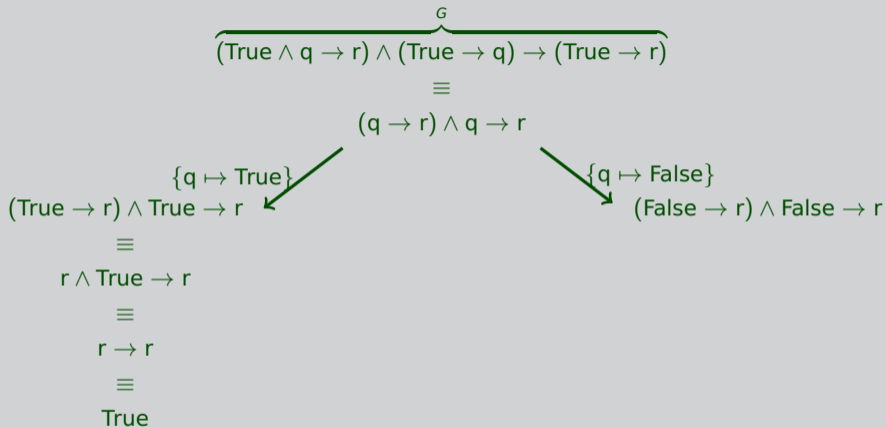
Beispiel (Fortsetzung)



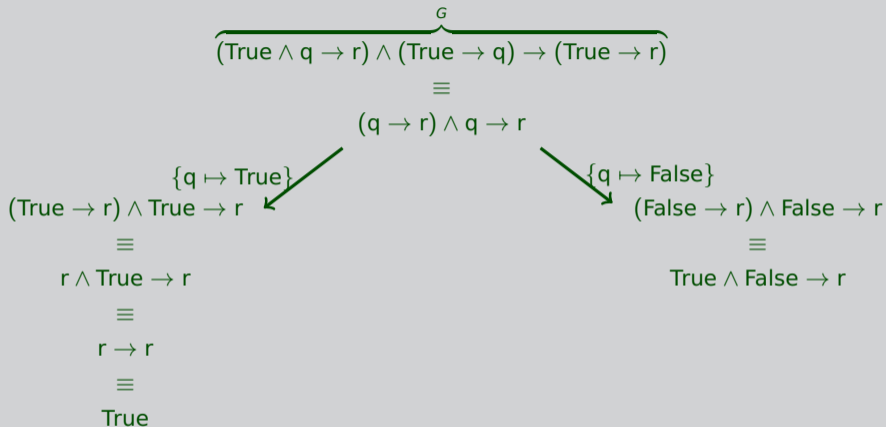
Beispiel (Fortsetzung)



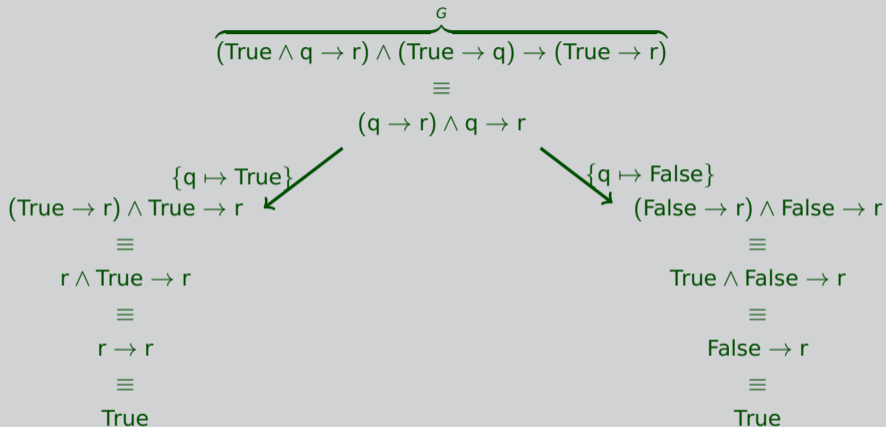
Beispiel (Fortsetzung)



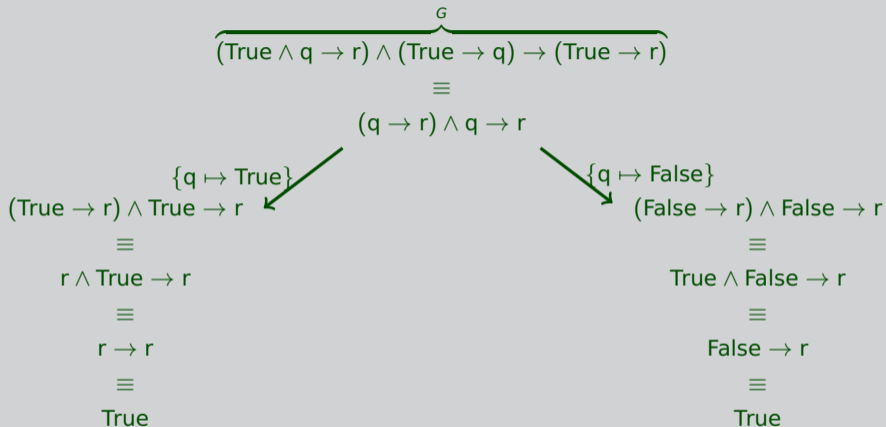
Beispiel (Fortsetzung)



Beispiel (Fortsetzung)



Beispiel (Fortsetzung)



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

Natürliches Schließen

Wintersemester 2022/23

Inferenzregeln: Konjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>	
\wedge	$\frac{A \quad B}{A \wedge B} \wedge: i$	$\frac{A \wedge B}{A} \wedge: e$	$\frac{A \wedge B}{B} \wedge: e$

Inferenzregeln: Konjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>	
\wedge	$\frac{A \quad B}{A \wedge B} \wedge: i$	$\frac{A \wedge B}{A} \wedge: e$	$\frac{A \wedge B}{B} \wedge: e$

Beispiel

Wir betrachten die folgenden Inferenzen, die wir etwa in informellen Beweisen verwendet haben:

$$\frac{p \rightarrow q \quad q \rightarrow p}{(p \rightarrow q) \wedge (q \rightarrow p)} \wedge: i \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{p \rightarrow q} \wedge: e \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{q \rightarrow p} \wedge: e$$

Inferenzregeln: Konjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>	
\wedge	$\frac{A \quad B}{A \wedge B} \wedge: i$	$\frac{A \wedge B}{A} \wedge: e$	$\frac{A \wedge B}{B} \wedge: e$

Beispiel

Wir betrachten die folgenden Inferenzen, die wir etwa in informellen Beweisen verwendet haben:

$$\frac{p \rightarrow q \quad q \rightarrow p}{(p \rightarrow q) \wedge (q \rightarrow p)} \wedge: i \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{p \rightarrow q} \wedge: e \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{q \rightarrow p} \wedge: e$$

Inferenzregeln: Konjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>	
\wedge	$\frac{A \quad B}{A \wedge B} \wedge: i$	$\frac{A \wedge B}{A} \wedge: e$	$\frac{A \wedge B}{B} \wedge: e$

Beispiel

Wir betrachten die folgenden Inferenzen, die wir etwa in informellen Beweisen verwendet haben:

$$\frac{p \rightarrow q \quad q \rightarrow p}{(p \rightarrow q) \wedge (q \rightarrow p)} \wedge: i \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{p \rightarrow q} \wedge: e \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{q \rightarrow p} \wedge: e$$

Inferenzregeln: Konjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>	
\wedge	$\frac{A \quad B}{A \wedge B} \wedge: i$	$\frac{A \wedge B}{A} \wedge: e$	$\frac{A \wedge B}{B} \wedge: e$

Beispiel

Wir betrachten die folgenden Inferenzen, die wir etwa in informellen Beweisen verwendet haben:

$$\frac{p \rightarrow q \quad q \rightarrow p}{(p \rightarrow q) \wedge (q \rightarrow p)} \wedge: i \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{p \rightarrow q} \wedge: e \quad \frac{(p \rightarrow q) \wedge (q \rightarrow p)}{q \rightarrow p} \wedge: e$$

Inferenzregeln: Disjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{A}{A \vee B} \vee:i$ $\frac{B}{A \vee B} \vee:i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \vdots \\ C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \vdots \\ C \\ \hline \end{array}}{C} \vee:e$

Inferenzregeln: Disjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{A}{A \vee B} \vee: i$ $\frac{B}{A \vee B} \vee: i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \hline \vdots \\ \hline C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \hline \vdots \\ \hline C \\ \hline \end{array}}{C} \vee: e$

Beispiel

$$\frac{p}{p \vee \neg p} \vee: i \quad \frac{\neg p}{p \vee \neg p} \vee: i \quad \frac{\text{True} \vee \text{False} \quad \begin{array}{|c|} \hline \text{True} \\ \hline \text{True} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \text{False} \\ \hline \text{True} \\ \hline \end{array}}{\text{True}} \vee: e$$

Inferenzregeln: Disjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{A}{A \vee B} \vee: i$ $\frac{B}{A \vee B} \vee: i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \hline \vdots \\ \hline C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \hline \vdots \\ \hline C \\ \hline \end{array}}{C} \vee: e$

Beispiel

$$\frac{p}{p \vee \neg p} \vee: i \quad \frac{\neg p}{p \vee \neg p} \vee: i \quad \frac{\text{True} \vee \text{False} \quad \begin{array}{|c|} \hline \text{True} \\ \hline \text{True} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \text{False} \\ \hline \text{True} \\ \hline \end{array}}{\text{True}} \vee: e$$

Inferenzregeln: Disjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{A}{A \vee B} \vee: i$ $\frac{B}{A \vee B} \vee: i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \hline \vdots \\ \hline C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \hline \vdots \\ \hline C \\ \hline \end{array}}{C} \vee: e$

Beispiel

$$\frac{p}{p \vee \neg p} \vee: i \quad \frac{\neg p}{p \vee \neg p} \vee: i \quad \frac{\text{True} \vee \text{False} \quad \begin{array}{|c|} \hline \text{True} \\ \hline \text{True} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \text{False} \\ \hline \text{True} \\ \hline \end{array}}{\text{True}} \vee: e$$

Inferenzregeln: Disjunktion

Definition

	<i>Einführung</i>	<i>Elimination</i>
\vee	$\frac{A}{A \vee B} \vee: i$ $\frac{B}{A \vee B} \vee: i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \hline \vdots \\ \hline C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \hline \vdots \\ \hline C \\ \hline \end{array}}{C} \vee: e$

Beispiel

$$\frac{p}{p \vee \neg p} \vee: i \quad \frac{\neg p}{p \vee \neg p} \vee: i \quad \frac{\text{True} \vee \text{False} \quad \begin{array}{|c|} \hline \text{True} \\ \hline \text{True} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \text{False} \\ \hline \text{True} \\ \hline \end{array}}{\text{True}} \vee: e$$

Inferenzregeln: Implikation

Definition

	<i>Einführung</i>	<i>Elimination</i>
\rightarrow	$\frac{\begin{array}{ l} A \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow : i$	$\frac{A \quad A \rightarrow B}{B} \rightarrow : e$

Inferenzregeln: Implikation

Definition

	<i>Einführung</i>	<i>Elimination</i>
\rightarrow	$\frac{\begin{array}{ l} A \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow: i$	$\frac{A \quad A \rightarrow B}{B} \rightarrow: e$

Beispiel

$$\frac{\begin{array}{|l} \text{False} \\ \text{True} \end{array}}{\text{False} \rightarrow \text{True}} \rightarrow: i$$

$$\frac{p \quad p \rightarrow q}{q} \rightarrow: e$$

Inferenzregeln: Implikation

Definition

	<i>Einführung</i>	<i>Elimination</i>
\rightarrow	$\frac{\begin{array}{ l} A \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow: i$	$\frac{A \quad A \rightarrow B}{B} \rightarrow: e$

Beispiel

$$\frac{\begin{array}{|l} \text{False} \\ \text{True} \end{array}}{\text{False} \rightarrow \text{True}} \rightarrow: i$$

$$\frac{p \quad p \rightarrow q}{q} \rightarrow: e$$

Inferenzregeln: Implikation

Definition

	<i>Einführung</i>	<i>Elimination</i>
\rightarrow	$\frac{\begin{array}{ l} A \\ \vdots \\ B \end{array}}{A \rightarrow B} \rightarrow : i$	$\frac{A \quad A \rightarrow B}{B} \rightarrow : e$

Beispiel

$$\frac{\begin{array}{|l} \text{False} \\ \text{True} \end{array}}{\text{False} \rightarrow \text{True}} \rightarrow : i$$

$$\frac{p \quad p \rightarrow q}{q} \rightarrow : e$$

Inferenzregeln: Negation et al.

Definition

	<i>Einführung</i>	<i>Elimination</i>
\neg	$\frac{\boxed{\begin{array}{c} A \\ \vdots \\ \text{False} \end{array}}}{\neg A} \neg: i$	$\frac{A \quad \neg A}{\text{False}} \neg: e$
False		$\frac{\text{False}}{A} \text{False}: e$
$\neg\neg$		$\frac{\neg\neg A}{A} \neg\neg: e$

Natürliches Schließen (alle Inferenzregeln)

	<i>Einführung</i>	<i>Elimination</i>
\wedge	$\frac{A \quad B}{A \wedge B} \wedge : i$	$\frac{A \wedge B}{A} \wedge : e \quad \frac{A \wedge B}{B} \wedge : e$
\vee	$\frac{A}{A \vee B} \vee : i \quad \frac{B}{A \vee B} \vee : i$	$\frac{A \vee B \quad \begin{array}{ c } \hline A \\ \vdots \\ C \\ \hline \end{array} \quad \begin{array}{ c } \hline B \\ \vdots \\ C \\ \hline \end{array}}{C} \vee : e$
\rightarrow	$\frac{\begin{array}{ c } \hline A \\ \vdots \\ B \\ \hline \end{array}}{A \rightarrow B} \rightarrow : i$	$\frac{A \quad A \rightarrow B}{B} \rightarrow : e$

	<i>Einführung</i>	<i>Elimination</i>
\neg	$\frac{\begin{array}{c} A \\ \vdots \\ \text{False} \end{array}}{\neg A} \quad \neg: i$	$\frac{A \quad \neg A}{\text{False}} \quad \neg: e$
False		$\frac{\text{False}}{A} \quad \text{False}: e$
$\neg\neg$		$\frac{\neg\neg A}{A} \quad \neg\neg: e$

	<i>Einführung</i>	<i>Elimination</i>
\neg	$\frac{\begin{array}{c} A \\ \vdots \\ \text{False} \end{array}}{\neg A} \quad \neg: i$	$\frac{A \quad \neg A}{\text{False}} \quad \neg: e$
False		$\frac{\text{False}}{A} \quad \text{False}: e$
$\neg\neg$		$\frac{\neg\neg A}{A} \quad \neg\neg: e$

Definition

Der Kalkül NK des **natürlichen Schließens** besteht aus den gerade betrachteten Beweisregeln.

Beweisbarkeitsrelation

Definition

Sei \mathcal{G} eine endliche Menge von Formeln und F eine Formel.

- Ein **Beweis von F aus \mathcal{G}** ist eine Folge von Formeln A_1, \dots, A_n mit $A_n = F$, sodass gilt: $A_i \in \mathcal{G}$ oder A_i folgt durch Anwendung einer der Regeln in NK.

Beweisbarkeitsrelation

Definition

Sei \mathcal{G} eine endliche Menge von Formeln und F eine Formel.

- Ein **Beweis von F aus \mathcal{G}** ist eine Folge von Formeln A_1, \dots, A_n mit $A_n = F$, sodass gilt: $A_i \in \mathcal{G}$ oder A_i folgt durch Anwendung einer der Regeln in NK.
- Eine Formel F heißt **beweisbar** aus den Annahmen \mathcal{G} , wenn es einen Beweis von F aus \mathcal{G} gibt.

Beweisbarkeitsrelation

Definition

Sei \mathcal{G} eine endliche Menge von Formeln und F eine Formel.

- Ein **Beweis von F aus \mathcal{G}** ist eine Folge von Formeln A_1, \dots, A_n mit $A_n = F$, sodass gilt: $A_i \in \mathcal{G}$ oder A_i folgt durch Anwendung einer der Regeln in NK.
- Eine Formel F heißt **beweisbar** aus den Annahmen \mathcal{G} , wenn es einen Beweis von F aus \mathcal{G} gibt.
- Ein Beweis wird oft auch als **Ableitung**, **Herleitung** oder **Deduktion** bezeichnet.

Beweisbarkeitsrelation

Definition

Sei \mathcal{G} eine endliche Menge von Formeln und F eine Formel.

- Ein **Beweis von F aus \mathcal{G}** ist eine Folge von Formeln A_1, \dots, A_n mit $A_n = F$, sodass gilt: $A_i \in \mathcal{G}$ oder A_i folgt durch Anwendung einer der Regeln in NK.
- Eine Formel F heißt **beweisbar** aus den Annahmen \mathcal{G} , wenn es einen Beweis von F aus \mathcal{G} gibt.
- Ein Beweis wird oft auch als **Ableitung**, **Herleitung** oder **Deduktion** bezeichnet.

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**.

Beispiel

Wir betrachten die folgende Tautologie

$$a \rightarrow (b \rightarrow (c \rightarrow (d \rightarrow (e \rightarrow c))))))$$

Beispiel

Wir betrachten die folgende Tautologie

$$a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$$

1	a	Prämisse
2	b	Prämisse
3	c	Prämisse
4	d	Prämisse
5	e	Prämisse
6	c	3
7	$e \rightarrow c$	5, 6, \rightarrow : i
8	$d \rightarrow e \rightarrow c$	4, 7, \rightarrow : i
9	$c \rightarrow d \rightarrow e \rightarrow c$	3, 8, \rightarrow : i
10	$b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$	2, 9, \rightarrow : i
11	$a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$	1, 10, \rightarrow : i

Beispiel

Wir betrachten die folgende Tautologie

$$a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$$

1	a	Prämisse
2	b	Prämisse
3	c	Prämisse
4	d	Prämisse
5	e	Prämisse
6	c	3
7	$e \rightarrow c$	5, 6, \rightarrow : i
8	$d \rightarrow e \rightarrow c$	4, 7, \rightarrow : i
9	$c \rightarrow d \rightarrow e \rightarrow c$	3, 8, \rightarrow : i
10	$b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$	2, 9, \rightarrow : i
11	$a \rightarrow b \rightarrow c \rightarrow d \rightarrow e \rightarrow c$	1, 10, \rightarrow : i

Versuchen Sie als Übung die Tautologie mit der Methode von Quine nachzuweisen.

Korrektheit und Vollständigkeit

Satz

Der Kalkül NK 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

Der Kalkül NK ist *korrekt* und *vollständig* für die Aussagenlogik:

$$A_1, \dots, A_n \models B \iff A_1, \dots, A_n \vdash B$$

Korrektheit und Vollständigkeit

Satz

Der Kalkül NK ist korrekt und *vollständig* für die Aussagenlogik:

$$A_1, \dots, A_n \models B \Rightarrow A_1, \dots, A_n \vdash B$$

Korrektheit und Vollständigkeit

Satz

Der Kalkül NK 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 \Rightarrow *SAT/SMT solvers*

Korrektheit und Vollständigkeit

Satz

Der Kalkül NK 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 \Rightarrow *SAT/SMT solvers*

Satz (Deduktionstheorem)

Gelte $A \vdash B$, dann existiert ein Beweis von $A \rightarrow B$, der A nicht als Prämisse hat

Beweis des Deduktionstheorems.

- Nach Annahme gilt $A_1, \dots, A_i, \dots, A_n \vdash B$.
- OBdA. können wir annehmen, dass $n = i$.

Beweis des Deduktionstheorems.

- Nach Annahme gilt $A_1, \dots, A_i, \dots, A_n \vdash B$.
- OBdA. können wir annehmen, dass $n = i$.
- Also gibt es einen Beweis in NK der folgenden Gestalt:

1	A_1	Prämisse
\vdots	\vdots	
$n - 1$	A_{n-1}	Prämisse
n	A_n	Prämisse
\vdots	\vdots	
k	B	

Beweis des Deduktionstheorems.

- Nach Annahme gilt $A_1, \dots, A_i, \dots, A_n \vdash B$.
- OBdA. können wir annehmen, dass $n = i$.
- Also gibt es einen Beweis in NK der folgenden Gestalt:

1	A_1	Prämisse
\vdots	\vdots	
$n - 1$	A_{n-1}	Prämisse
n	A_n	Prämisse
\vdots	\vdots	
k	B	

- Nun fügen wir diesem Beweis eine Anwendung der $\rightarrow : i$ Regel auf die Formeln A_n und B hinzu, wodurch aus der Prämisse A_n eine (lokale) Annahme wird.

Beweis (Fortsetzung).

- Wir erhalten einen Beweis von $A_n \rightarrow B$:

1	A_1	Prämisse
\vdots	\vdots	
$n - 1$	A_{n-1}	Prämisse
n	A_n	Annahme
\vdots	\vdots	
k	B	
$k + 1$	$A_n \rightarrow B$	$\rightarrow: i$

Beweis (Fortsetzung).

- Wir erhalten einen Beweis von $A_n \rightarrow B$:

1	A_1	Prämisse
\vdots	\vdots	
$n - 1$	A_{n-1}	Prämisse
n	A_n	Annahme
\vdots	\vdots	
k	B	
$k + 1$	$A_n \rightarrow B$	$\rightarrow: i$

- Somit ist die Prämisse A_n aus der Liste der Annahmen eliminiert und wir haben im Allgemeinen die Korrektheit des folgenden Sequents nachgewiesen:

$$A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_n \vdash A_i \rightarrow B .$$

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg: e$
3	$\neg\neg p \rightarrow p$	1, 2, $\rightarrow: i$

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg: e$
3	$\neg\neg p \rightarrow p$	1, 2, $\rightarrow: i$

Folgerung

- Die Formel $\neg\neg p \rightarrow p$ ist eine Tautologie.

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg: e$
3	$\neg\neg p \rightarrow p$	1, 2, $\rightarrow: i$

Folgerung

- Die Formel $\neg\neg p \rightarrow p$ ist eine Tautologie.
- Die Formel $\neg\neg p \rightarrow p$ ist formal beweisbar.

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg: e$
3	$\neg\neg p \rightarrow p$	1, 2, $\rightarrow: i$

Folgerung

- Die Formel $\neg\neg p \rightarrow p$ ist eine Tautologie.
- Die Formel $\neg\neg p \rightarrow p$ ist formal beweisbar.
- Wegen Korrektheit und Vollständigkeit gilt die folgende Äquivalenz:

$$\neg\neg p \models p \quad \text{gdw.} \quad \neg\neg p \vdash p$$

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \rightarrow p$$

1	$\neg\neg p$	Prämisse
2	p	$\neg\neg: e$
3	$\neg\neg p \rightarrow p$	1, 2, $\rightarrow: i$

Folgerung

- Die Formel $\neg\neg p \rightarrow p$ ist eine Tautologie.
- Die Formel $\neg\neg p \rightarrow p$ ist formal beweisbar.
- Wegen Korrektheit und Vollständigkeit gilt die folgende Äquivalenz:

$$\neg\neg A \models A \quad \text{gdw.} \quad \neg\neg A \vdash A$$