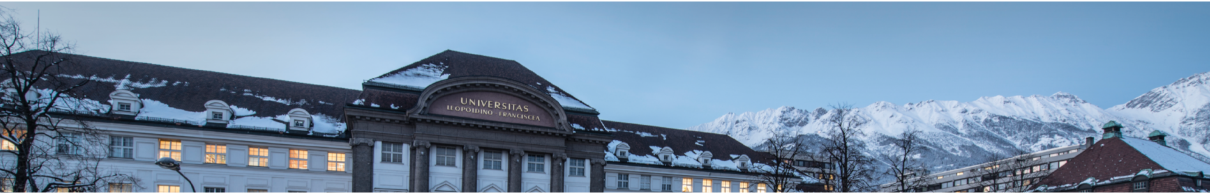
universität
innsbruck

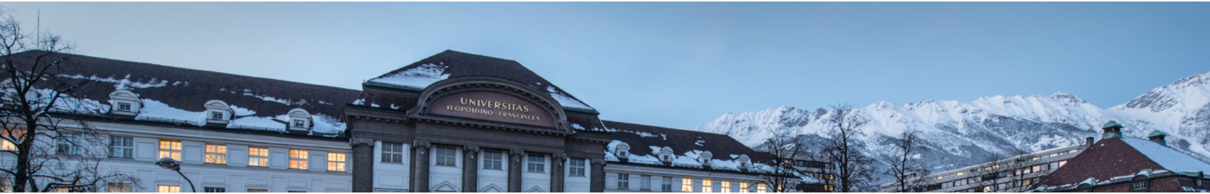


Einführung in die Theoretische Informatik

Martin Avanzini Christian Dalvit Jamie Hochrainer
Georg Moser Johannes Niederhauser Jonas Schöpf

https://tcs-informatik.uibk.ac.at

universität innsbruck



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

$$\neg A \qquad (A \land B) \qquad (A \lor B) \qquad (A \to B)$$

auch Formeln

Definitionen

- Erweiterung der Belegung v zu einem Wahrheitswert $\overline{\mathrm{v}}$ 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

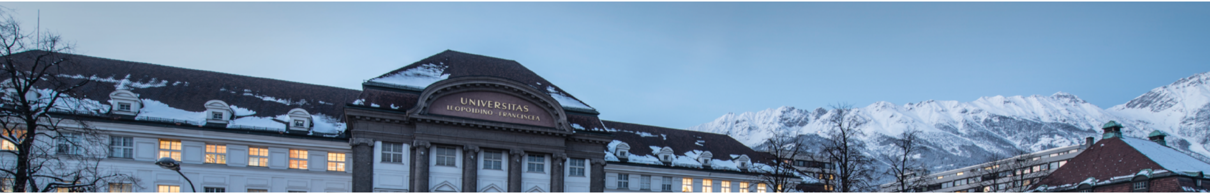
Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen, Chomsky-Hierarchie, Anwendungen von formalen Sprachen

Einführung in die Berechenbarkeitstheorie und Komplexitätstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen, Komplexitätstheorie

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare



Methode von Quine

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

1. *A ist eine Tautologie gdw.*

$$A\{p \mapsto \mathrm{True}\} \textit{ ist Tautologie} \quad \textit{und} \quad A\{p \mapsto \mathrm{False}\} \textit{ ist Tautologie}$$

2. *A ist unerfüllbar gdw.*

$$A\{p \mapsto \mathrm{True}\} \textit{ unerfüllbar} \quad \textit{und} \quad A\{p \mapsto \mathrm{False}\} \textit{ unerfüllbar}$$

Beispiel (Wahrheitstabellen oder logische Äquivalenzen)

Wir betrachten die Formel F

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

Es ist nicht schwer einzusehen, dass F eine Tautologie ist

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

1. $(\mathsf{True} \wedge q \to r) \wedge (\mathsf{True} \to q) \to (\mathsf{True} \to r) =: G$ ist Tautologie
2. $(\mathsf{False} \wedge q \to r) \wedge (\mathsf{False} \to q) \to (\mathsf{False} \to r)$ ist Tautologie

Anforderungen in Baumform:

$$(p \wedge q \to r) \wedge (p \to q) \to (p \to r)$$

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

$$G$$

$\{p \mapsto \mathsf{False}\}$:

$$\begin{gathered}(\mathsf{False} \wedge q \to r) \wedge (\mathsf{False} \to q) \to (\mathsf{False} \to r) \\ \equiv \\ (\mathsf{False} \to r) \wedge (\mathsf{False} \to q) \to \mathsf{True} \\ \equiv \\ \mathsf{True} \wedge \mathsf{True} \to \mathsf{True} \\ \equiv \\ \mathsf{True}\end{gathered}$$

Übrige Anforderungen

3. G ist Tautologie

Beispiel (Fortsetzung)

$$\overbrace{(\mathsf{True} \wedge q \to r) \wedge (\mathsf{True} \to q) \to (\mathsf{True} \to r)}^{G}$$

$$\equiv$$

$$(q \to r) \wedge q \to r$$

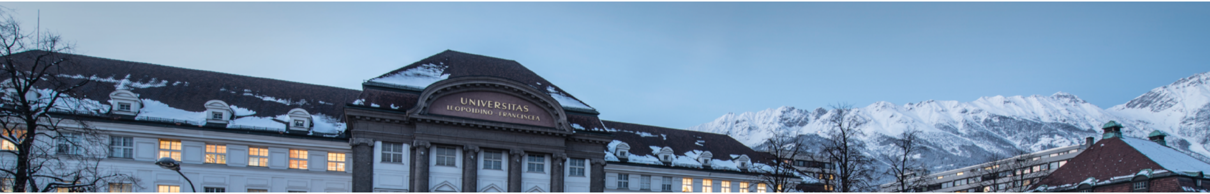
$\{q \mapsto \mathsf{True}\}$

$$(\mathsf{True} \to r) \wedge \mathsf{True} \to r \equiv r \wedge \mathsf{True} \to r \equiv r \to r \equiv \mathsf{True}$$

$\{q \mapsto \mathsf{False}\}$

$$(\mathsf{False} \to r) \wedge \mathsf{False} \to r \equiv \mathsf{True} \wedge \mathsf{False} \to r \equiv \mathsf{False} \to r \equiv \mathsf{True}$$

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



Natürliches Schließen

Inferenzregeln: Konjunktion

Definition

	Einführung	*Elimination*
$\wedge$	$\dfrac{A \quad B}{A \wedge B}\ \wedge\colon \mathrm{i}$	$\dfrac{A \wedge B}{A}\ \wedge\colon \mathrm{e} \qquad \dfrac{A \wedge B}{B}\ \wedge\colon \mathrm{e}$

Beispiel

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

$$\frac{p \to q \quad q \to p}{(p \to q) \wedge (q \to p)}\ \wedge\colon \mathrm{i} \qquad \frac{(p \to q) \wedge (q \to p)}{p \to q}\ \wedge\colon \mathrm{e} \qquad \frac{(p \to q) \wedge (q \to p)}{q \to p}\ \wedge\colon \mathrm{e}$$

Inferenzregeln: Disjunktion

Definition

	Einführung	*Elimination*
$\vee$	$\dfrac{A}{A \vee B}\ \vee{:}\,\mathrm{i} \qquad \dfrac{B}{A \vee B}\ \vee{:}\,\mathrm{i}$	$\dfrac{A \vee B \quad \boxed{\begin{matrix} A \\ \vdots \\ C \end{matrix}} \quad \boxed{\begin{matrix} B \\ \vdots \\ C \end{matrix}}}{C}\ \vee{:}\,\mathrm{e}$

Beispiel

$$\frac{p}{p \vee \neg p}\ \vee{:}\,\mathrm{i} \qquad \frac{\neg p}{p \vee \neg p}\ \vee{:}\,\mathrm{i} \qquad \frac{\mathsf{True} \vee \mathsf{False} \quad \boxed{\begin{matrix} \mathsf{True} \\ \mathsf{True} \end{matrix}} \quad \boxed{\begin{matrix} \mathsf{False} \\ \mathsf{True} \end{matrix}}}{\mathsf{True}}\ \vee{:}\,\mathrm{e}$$

Inferenzregeln: Implikation

Definition

	Einführung	*Elimination*
$\rightarrow$	$\dfrac{\boxed{\begin{array}{l} A \\ \vdots \\ B \end{array}}}{A \rightarrow B}$ $\rightarrow$: i	$\dfrac{A \quad A \rightarrow B}{B}$ $\rightarrow$: e

Beispiel

$\dfrac{\boxed{\begin{array}{l} \text{False} \\ \text{True} \end{array}}}{\text{False} \rightarrow \text{True}}$ $\rightarrow$: i

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

Inferenzregeln: Negation et al.

Definition

	Einführung	*Elimination*
$\neg$	$\dfrac{\boxed{\begin{array}{l} A \\ \vdots \\ \mathrm{False} \end{array}}}{\neg A}\ \neg\colon \mathrm{i}$	$\dfrac{A \quad \neg A}{\mathrm{False}}\ \neg\colon \mathrm{e}$
False		$\dfrac{\mathrm{False}}{A}\ \mathrm{False}\colon \mathrm{e}$
$\neg\neg$		$\dfrac{\neg\neg A}{A}\ \neg\neg\colon \mathrm{e}$

Natürliches Schließen (alle Inferenzregeln)

	Einführung	*Elimination*
$\wedge$	$\dfrac{A \quad B}{A \wedge B}\ \wedge: \mathrm{i}$	$\dfrac{A \wedge B}{A}\ \wedge: \mathrm{e} \qquad \dfrac{A \wedge B}{B}\ \wedge: \mathrm{e}$
$\vee$	$\dfrac{A}{A \vee B}\ \vee: \mathrm{i} \qquad \dfrac{B}{A \vee B}\ \vee: \mathrm{i}$	$\dfrac{A \vee B \quad \boxed{\begin{array}{c} A \\ \vdots \\ C \end{array}} \quad \boxed{\begin{array}{c} B \\ \vdots \\ C \end{array}}}{C}\ \vee: \mathrm{e}$
$\rightarrow$	$\dfrac{\boxed{\begin{array}{c} A \\ \vdots \\ B \end{array}}}{A \rightarrow B}\ \rightarrow: \mathrm{i}$	$\dfrac{A \quad A \rightarrow B}{B}\ \rightarrow: \mathrm{e}$

	Einführung	*Elimination*
$\neg$	$$\dfrac{\boxed{\begin{array}{l} A \\ \vdots \\ \mathsf{False} \end{array}}}{\neg A}\ \neg: \mathrm{i}$$	$$\dfrac{A \quad \neg A}{\mathsf{False}}\ \neg: \mathrm{e}$$
False		$$\dfrac{\mathsf{False}}{A}\ \mathsf{False}: \mathrm{e}$$
$\neg\neg$		$$\dfrac{\neg\neg A}{A}\ \neg\neg: \mathrm{e}$$

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 $A_1, \ldots, A_n$ 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 $A_1, \ldots, A_n \vdash B$ gilt, gdw. B aus $A_1, \ldots, A_n$ beweisbar ist.
2. Wir schreiben $\vdash A$ statt $\varnothing \vdash A$ und nennen A in diesem Fall beweisbar.

Beispiel

Wir betrachten die folgende Tautologie

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

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

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

Korrektheit und Vollständigkeit

Satz

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

$$A_1, \ldots, A_n \models B \quad \textit{gdw.} \Longleftrightarrow \quad A_1, \ldots, A_n \vdash B$$

∎

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* $A \to B$, *der* A *nicht als Prämisse hat*

Beweis des Deduktionstheorems.

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

$$
\begin{array}{rll}
1 & A_1 & \text{Prämisse} \\
\vdots & \vdots & \\
n-1 & A_{n-1} & \text{Prämisse} \\
n & A_n & \text{Prämisse} \\
\vdots & \vdots & \\
k & B &
\end{array}
$$

- 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 $A_n \to B$:

$$
\begin{array}{rl|ll|}
1 & & A_1 & \text{Prämisse} & \\
\vdots & & \vdots & & \\
n-1 & & A_{n-1} & \text{Prämisse} & \\
\cline{2-5}
n & & A_n & \text{Annahme} & \\
\vdots & & \vdots & & \\
k & & B & & \\
\cline{2-5}
k+1 & & A_n \to B & \to: \mathrm{i} &
\end{array}
$$

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

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

Beispiel

Wir betrachten die formale Ableitung der Formel

$$\neg\neg p \to p$$

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

Folgerung

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

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