universität innsbruck

Einführung in die Theoretische Informatik

David Drexel, Julian Fodor, Alexander Lochmann, **Georg Moser**, Alexander Maringele, David Obwaller, Jonas Schöpf

cbr.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

$$\neg A \qquad (A \wedge B) \qquad (A \vee B) \qquad (A \to B)$$

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

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:

„more formal souvereignty" $\to$ „less real souvereignty" $\models$
$\models \neg$„more formal souvereignty" $\to \neg$„less real souvereignty"

[1] Paul 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

Methode von Quine

Lemma

A eine Formel und p ein Atom in A

1. *A ist eine Tautologie gdw.*

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

2. *A ist unerfüllbar gdw.*

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

Beispiel (Wahrheitstabellen oder logische Äquivalenzen)

Wir betrachten die Formel F

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

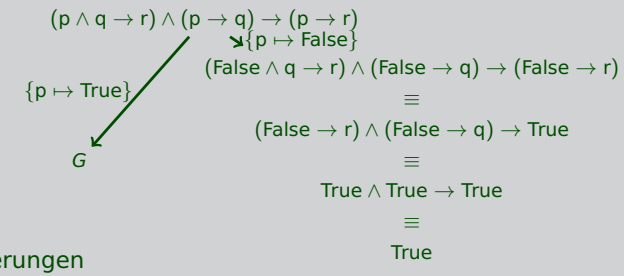
Es ist nicht schwer einzusehen, dass F eine Tautologie ist

Beispiel (Methode von Quine)

Die Methode liefert die folgenden Anforderungen

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

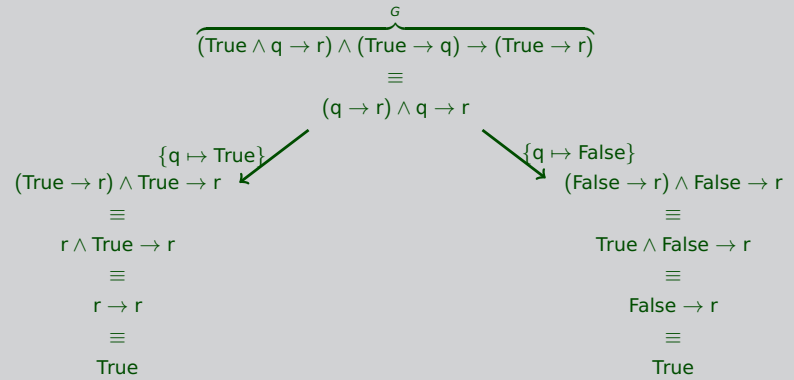
Anforderungen in Baumform:



Übrige Anforderungen

3. G ist Tautologie

Beispiel (Fortsetzung)



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

Formales Beweisen

Modus Ponens

$$\frac{A \to B \quad A}{B}\ MP$$

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

(1) $A \to (B \to A)$

(2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(3) $(\neg A \to \neg B) \to (B \to A)$

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

1. Ein Beweis von F aus $\mathcal{G}$ ist eine Sequenz
$$A_1, \ldots, A_n = F$$
sodass für alle $1 \leqslant i \leqslant n$:
   - $A_i \in \mathcal{G}$
   - 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 $A_1, \ldots, A_n \vdash B$ 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

Korrektheit und Vollständigkeit

Satz

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

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

Fakt

Basierend auf einem korrekten und vollständigen Beweissystem können wir versuchen das Beweisen zu automatisieren $\to$ SAT solvers

Satz (Deduktionstheorem)

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

Beispiel

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

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

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

Nun zeigen wir die Gültigkeit mit folgenden Beweis:

1	$\neg p$	Prämisse
2	$\neg p \to (\neg q \to \neg p)$	Axiom (1)
3	$\neg q \to \neg p$	1, 2, *Modus Ponens*
4	$(\neg q \to \neg p) \to (p \to q)$	Axiom (3)
5	$p \to q$	3, 4, *Modus Ponens*
6	$\neg p \to (p \to q)$	1, 5, *Deduktionstheorem*

Beweis des Deduktionstheorems.

Angenommen B wird mit dem Beweis

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

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

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

1. Basis: $k = 1$; dann gilt $B_1 = A$ und die Behauptung, da $A \to A$ beweisbar
2. Schritt: $k > 1$; die Induktionshypothese besagt

   Für alle $l < k$ ist $A \to B_l$ 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, $B_j = (B_i \to B_k)$

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	$B_k \to (A \to B_k)$	Axiom (1)
3	$A \to B_k$	1, 2, MP

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

  Wir verwenden folgenden Beweis:

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

Definition

Eine Wahrheitsfunktion $f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ ist eine Funktion, die n Wahrheitswerten einen Wahrheitswert zuordnet

Definition

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

$$\mathrm{TV}(f) := \{(s_1, \ldots, s_n) \mid f(s_1, \ldots, s_n) = \mathsf{T}\}$$

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

Lemma

- *$f\colon \{\mathsf{T},\mathsf{F}\}^n \to \{\mathsf{T},\mathsf{F}\}$ eine Wahrheitsfunktion*
  $\mathrm{TV}(f) \neq \varnothing$, $\mathrm{TV}(f) \neq \{\mathsf{T},\mathsf{F}\}^n$
- *$p_1, \ldots, p_n$ atomare Formeln*
- *Sei DNF D definiert als:*

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

  wobei $A_i = p_i$, wenn $s_i = \mathsf{T}$ und $A_i = \neg p_i$ sonst
- *Sei KNF K definiert als:*

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

  wobei $B_j = \neg p_j$, wenn $s_j = \mathsf{T}$ und $B_j = p_j$ sonst
- *Die Wahrheitstabellen von D und K entsprechen der Wahrheitsfunktion f*

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:
   - $\mathrm{TV}(f) = \varnothing$
   - $\mathrm{TV}(f) = \{\mathsf{T}, \mathsf{F}\}^n$
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

Wir erstellen die KNF.

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

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