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

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

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

Definition

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

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

Beispiel (Wiederholung)

Wir betrachten die 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

Beispiel

Wir betrachten die Ableitung der Umkehrung

$p \to \neg\neg p$ → ersetzen durch A, B, ...

1	p	Prämisse
2	$\neg p$	Prämisse
3	False	1, 2, $\neg$: e
4	$\neg\neg p$	2,3, $\neg$: i

Beispiel (Abgeleitete Regel $\neg\neg$: i)

Mit der selben Ableitung erhalten wir die folgende (abgeleitete) Inferenzregel:

$$\frac{A}{\neg\neg A}\ \neg\neg\text{: i}$$

NB: Wir schreiben Inferenzregeln immer mit den Metavariablen für Formeln A, B, C ...

Beispiel

Wir betrachten noch eine weitere abgeleitete Inferenzregel, nämlich den Widerspruchsbeweis (WB):

$$\frac{\begin{array}{|l}\neg A\\ \vdots\\ \text{False}\end{array}}{A}\ \text{WB}$$

Beispiel (Abgeleitete Regel WB)

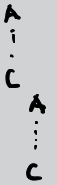
Die Ableitung der Regel WB gelingt wie folgt:

1	$\neg A \to \text{False}$	Prämisse, $\to$: i
2	$\neg A$	Prämisse
3	False	1, 2, $\to$: e
4	$\neg\neg A$	2,3,$\neg$: i
5	A	4,$\neg\neg$: e

Beispiel

Nun wollen wir noch $p \vee q \vdash q \vee p$ zeigen:

1	$p \vee q$	Prämisse
2	p A	Prämisse
3	$q \vee p$	2, $\vee$: i
4	q A	Prämisse
5	$q \vee p$	4, $\vee$: i
6	$q \vee p$	1,2-3,4-5, $\vee$: e



Diskurs: Axiome für die Aussagenlogik nach Frege und Łukasiewicz

- Der Kalkül NK des natürlichen Schließens ist (beileibe) nicht der einzige korrekte und vollständige Kalkül für die Aussagenlogik.

Definition

Axiome für die Aussagenlogik nach Frege und Łukasiewicz

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

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

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

Satz

Das Axiomensystem nach Frege und Łukasiewicz mit Inferenzregel Modus Ponens ist korrekt und vollständig für die Aussagenlogik. ■

universität
innsbruck

Konjunktive und Disjunktive Normalformen

Definition

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

boolesche Funktion

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.

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

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

universität
innsbruck

Algebraische Strukturen

Definition (Algebra)

Eine Algebra $\mathcal{A} = \langle A_1, \ldots, A_n; \circ_1, \ldots, \circ_m \rangle$ besteht aus

1. Träger (oder Trägermengen) $A_1, \ldots, A_n$
2. Operationen $\circ_1, \ldots, \circ_m$ auf den Trägern

Nullstellige Operationen werden auch Konstanten genannt; wir fixieren eine unendliche Menge von Variablen $x_1, x_2, \ldots$ und für jede Operation $\circ_i$ der Algebra $\mathcal{A}$ ein Symbol $\circ_i$ der gleichen Stelligkeit

Definition (Algebraische Ausdrücke)

Wir definieren die algebraischen Ausdrücke einer Algebra $\mathcal{A}$ induktiv:

1. Konstanten und Variablen sind algebraische Ausdrücke.
2. Wenn $A_1, \ldots, A_n$ algebraische Ausdrücke, $\circ$ eine Operation, dann ist $\circ(A_1, \ldots, A_n)$ ein algebraischer Ausdruck

Definition

Seien A und B algebraische Ausdrücke

- A und B sind äquivalent, wenn $\forall$ Instanzen A' und B' gilt: $A' = B'$
- Wenn A äquivalent zu B ist, schreiben wir kurz $A \approx B$

Definition

Wenn die Träger von $\mathcal{A}$ endlich sind, dann nennen wir $\mathcal{A}$ endlich

Beispiel

Sei $A = \{a, b, c, d\}$ und $\circ$ durch folgende Operationstabelle definiert:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Nullelement, neutrales Element, Inverses

Definition

Sei $\circ$ eine binäre Operation auf A

- Wenn $0 \in A$ existiert, sodass für alle $a \in A$

$$a \circ 0 = 0 \circ a = 0$$

  dann heißt 0 Nullelement für $\circ$

- Wenn $1 \in A$ existiert, sodass für alle $a \in A$

$$a \circ 1 = 1 \circ a = a$$

  dann heißt 1 Einselement (neutrales Element) für $\circ$

- Sei 1 das neutrale Element für $\circ$ und für $a \in A$, existiert $b \in A$, sodass

$$a \circ b = b \circ a = 1$$

  Dann heißt b das Inverse (Komplement) von a

Halbgruppen, Monoide und Gruppen

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ \rangle$ heißt

- Halbgruppe, wenn $\circ$ assoziativ
- Monoid, wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ eine Halbgruppe mit Einselement 1 für $\circ$
- Gruppe, wenn $\mathcal{A}$ ein Monoid ist und jedes Element ein Inverses hat

Eine Halbgruppe, ein Monoid oder eine Gruppe heißt kommutativ, wenn $\circ$ kommutativ

Beispiel

Die im vorigen Beispiel definierte Algebra $\mathcal{A}$ hat folgende Eigenschaften:

1. a ist das neutrale Element von $\circ$
2. Jedes Element besitzt ein Inverses
3. $\circ$ ist nicht kommutativ

Eigenschaft des neutralen Elements

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Beweis.

1. Sei $\circ$ eine binäre Operation auf der Menge A
2. Angenommen e und u sind neutrale Elemente für $\circ$
3. Wir zeigen, dass $e = u$

$$
\begin{aligned}
e &= e \circ u && \text{da } u \text{ Einselement} \\
&= u && \text{da } e \text{ Einselement}
\end{aligned}
$$

Eigenschaft des Inversen

Lemma

Wenn $\mathcal{A} = \langle A; \circ, 1 \rangle$ ein Monoid ist, dann ist das Inverse eindeutig

Beweis.

Sei $a \in A$ und seien b, c Inverse von a. Wir zeigen $b = c$:

$$
\begin{aligned}
b &= b \circ 1 && \text{1 ist neutrales Element} \\
&= b \circ (a \circ c) && c \text{ ist Komplement von } a \\
&= (b \circ a) \circ c && \text{Assoziativität von } \circ \\
&= 1 \circ c && b \text{ ist Komplement von } a \\
&= c && \text{1 ist neutrales Element}
\end{aligned}
$$

Ringe und Körper

Definition (Ring)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Ring, wenn

1. $\langle A; +, 0 \rangle$ eine kommutative Gruppe
2. $\langle A; \cdot, 1 \rangle$ ein Monoid
3. $\cdot$ distributiert über $+$ (von links und von rechts),
   das heißt für alle $a, b, c \in A$ gilt:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad (b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Definition (Körper)

Eine Algebra $\mathcal{A} = \langle A; +, \cdot, 0, 1 \rangle$ heißt Körper, wenn

1. $\mathcal{A}$ ein Ring
2. $\langle A \setminus \{0\}; \cdot, 1 \rangle$ eine kommutative Gruppe