

Einführung in die Theoretische Informatik

Woche 4

Harald Zankl

Institut für Informatik © UIBK
Wintersemester 2014/2015



Zusammenfassung der letzten LV

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

Satz

Das Axiomensystem mit Inferenzregel MP ist vollständig und korrekt für die Aussagenlogik: $A_1, \dots, A_n \models B$ gdw. $A_1, \dots, A_n \vdash B$

Konjunktive und Disjunktive Normalformen

Definition

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

Definition

- 1 Formel A ist in **konjunktiver Normalform (KNF)**, wenn A eine Konjunktion von Disjunktionen von Literalen ist
- 2 Formel A ist in **disjunktiver Normalform (DNF)**, wenn A eine Disjunktion von Konjunktionen von Literalen ist

Folgerung

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

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, Verschlüsselung und Sicherheit

Algebraische Strukturen

Definition (Algebra)

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

- 1 **Trägern** (oder **Trägermengen**) A_1, \dots, A_n
- 2 **Operationen** \circ_1, \dots, \circ_m auf den Trägern

Beispiel

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und \bullet gegeben durch:

\bullet	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

Definition (Algebraische Ausdrücke)

Sei \mathcal{A} eine Algebra. Nullstellige Operationen werden auch **Konstanten** genannt. Wir fixieren eine unendliche Menge von **Variablen** x_1, x_2, \dots und definieren **algebraische Ausdrücke** einer Algebra \mathcal{A} induktiv:

- 1 Konstanten und Variablen sind algebraische Ausdrücke.
- 2 Wenn E_1, \dots, E_n algebraische Ausdrücke und \circ eine Operation, dann ist $\circ(E_1, \dots, E_n)$ ein algebraischer Ausdruck.

Beispiel (Algebraische Ausdrücke)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$

$$x_1 \checkmark \quad a \checkmark \quad b \times \quad \bullet(x_1, x_2) \checkmark \quad x_1 \bullet x_2 \checkmark \quad a \bullet b \times \quad a \bullet (x_3 \bullet a) \checkmark$$

Definition (Äquivalenz)

Seien E und F algebraische Ausdrücke einer Algebra \mathcal{A} .

- Ersetzen von Variablen in E durch Werte aus Träger liefert **Instanz** E' .
- E und F sind **äquivalent**, wenn für alle Instanzen E' und F' deren Auswertung in \mathcal{A} übereinstimmt (wobei gleiche Variablen durch gleiche Werte ersetzt werden).
- Wenn E äquivalent zu F ist, schreiben wir kurz $E \approx F$.

Beispiel (Äquivalenz)

Sei Algebra $\mathcal{A} = \langle A; \bullet, a \rangle$ mit $A = \{a, b, c, d\}$ und \bullet gegeben durch:

\bullet	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	c
d	d	a	b	c

$$x_1 \approx a \quad \times \quad x_1 \approx x_1 \bullet x_2 \quad \times \quad x_1 \approx a \bullet (x_1 \bullet a) \quad \checkmark \quad a \approx a \bullet (x_1 \bullet a) \quad \times \quad x_1 \bullet x_2 \approx a \bullet (x_3 \bullet a) \quad \times$$

Nullelement, neutrales Element, Inverses

Definition

Sei \circ eine binäre Operation auf A

- $0 \in A$ heißt **Nullelement** für \circ , wenn
für alle $a \in A$ gilt $a \circ 0 = 0 \circ a = 0$
- $1 \in A$ heißt **Einselement (neutrales Element)** für \circ , wenn
für alle $a \in A$ gilt $a \circ 1 = 1 \circ a = a$
- $b \in A$ heißt **Inverses** von a , wenn 1 das neutrale Element für \circ und
 $a \circ b = b \circ a = 1$

Bemerkung

Nullelement, Einselement, bzw. Inverses existieren nicht immer.

Beispiel (Algebra \mathcal{A} bezüglich \bullet)

Nullelement: \times Einselement: a Inverses von $a/b/c/d$ ist $a/d/c/b$

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 $e = u$

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



Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

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

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen **kommutativ**, wenn \circ kommutativ ist.

Beispiel (Algebra \mathcal{A})

- 1 • ist nicht assoziativ, da z.B. $d \bullet (d \bullet d) \neq (d \bullet d) \bullet d$
- 2 $\rightarrow \langle A, \bullet \rangle$ ist keine Halbgruppe
- 3 $\rightarrow \langle A, \bullet, a \rangle$ ist kein Monoid
- 4 $\rightarrow \langle A, \bullet, a \rangle$ ist keine Gruppe
- 5 • ist nicht kommutativ, da z.B. $c \bullet d \neq d \bullet c$

Halbgruppen, Monoide und Gruppen

Definition

Sei $\mathcal{A} = \langle A; \circ \rangle$ eine Algebra. Dann heißt

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

Eine Halbgruppe, ein Monoid bzw. eine Gruppe heißen **kommutativ**, wenn \circ kommutativ ist.

Beispiel

- Halbgruppe: $\langle \mathbb{N}, + \rangle$ ✓ $\langle \mathbb{N}, \times \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ ✓
- Monoid: $\langle \mathbb{N}, +, 0 \rangle$ ✓ $\langle \mathbb{N}, \times, 1 \rangle$ ✓ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓
- Gruppe: $\langle \mathbb{N}, +, 0 \rangle$ ✗ $\langle \mathbb{N}, \times, 1 \rangle$ ✗ $\langle \mathbb{Q} \setminus \{0\}, \times, 1 \rangle$ ✓

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 $b = c$:

$$b = b \circ 1$$

$$= b \circ (a \circ c)$$

$$= (b \circ a) \circ c$$

$$= 1 \circ c$$

$$= c$$

1 ist neutrales Element

c ist Inverses von a

Assoziativität von \circ

b ist Inverses von a

1 ist neutrales Element



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 distribuiert über $+$ (von links und von rechts),
das heißt für alle $a, b, c \in A$ gilt:

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

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

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \bar{}, 0, 1 \rangle$ heißt **Boolesche Algebra** wenn gilt:

- 1 $\langle B; +, 0 \rangle$ und $\langle B; \cdot, 1 \rangle$ sind kommutative Monoide
- 2 Die Operationen $+$ und \cdot distribuieren übereinander. Es gilt also für alle $a, b, c \in B$:

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

- 3 Für alle $a \in B$ gilt

$$a + \bar{a} = 1 \quad a \cdot \bar{a} = 0$$

Das Element \bar{a} heißt das **Komplement** oder die **Negation** von a

Konventionen

- Wir lassen \cdot oft weg und schreiben ab statt $a \cdot b$
- Wir verwenden die folgende Präzedenz:
Komplement ($\bar{}$) bindet am stärksten, und \cdot bindet stärker als $+$

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen x_1, x_2, \dots gegeben; diese Variablen heißen **Boolesche Variablen**

Wir definieren **Boolesche Ausdrücke** induktiv:

- 1 0, 1 und Boolesche Variablen sind Boolesche Ausdrücke
- 2 Wenn A und B Boolesche Ausdrücke sind, dann sind

$$\bar{A} \quad (A \cdot B) \quad (A + B)$$

Boolesche Ausdrücke

Beispiel

Die folgenden Ausdrücke sind Boolesche Ausdrücke:

$$x_1 \quad x_2 \quad x_1 + x_2 \quad x_1 \cdot x_2 \quad x_1 \cdot (x_1 + x_2) \quad x_1(x_1 + x_2) \quad x_1 \overline{(x_1 + x_2)}$$

Mengenalgebra

Sei M eine Menge; $\mathcal{P}(M)$ bezeichnet die **Potenzmenge** von M , also

$$\mathcal{P}(M) := \{N \mid N \subseteq M\}$$

Definition

Wir betrachten die Algebra

$$\langle \mathcal{P}(M); \cup, \cap, \bar{}, \emptyset, M \rangle$$

- 1 \cup die Mengenvereinigung
- 2 \cap die Schnittmenge
- 3 $\bar{}$ die Komplementärmenge (bezüglich M)

Diese Algebra nennt man **Mengenalgebra**.

► Definitionen

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Binäre Algebra

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$

Definition

Wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, -, 0, 1 \rangle$$

wobei die Operationen $+$, \cdot , $-$ wie folgt definiert:

$$\begin{array}{c|cc}
 + & 1 & 0 \\
 \hline
 1 & 1 & 1 \\
 0 & 1 & 0
 \end{array}
 \quad
 \begin{array}{c|cc}
 \cdot & 1 & 0 \\
 \hline
 1 & 1 & 0 \\
 0 & 0 & 0
 \end{array}
 \quad
 \begin{array}{c|c}
 - & \\
 \hline
 1 & 0 \\
 0 & 1
 \end{array}$$

Diese Algebra nennt man **binäre Algebra**

Lemma

Die binäre Algebra ist eine Boolesche Algebra

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra \mathcal{Frm}

$$\langle \text{Frm}; \vee, \wedge, \neg, \text{False}, \text{True} \rangle$$

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden

Lemma

Die Algebra \mathcal{Frm} ist eine Boolesche Algebra

Mengenoperationen

Definition

Seien A und B Mengen. Dann ist

- $A \cap B := \{x \in A \text{ und } x \in B\}$
- $A \cup B := \{x \in A \text{ oder } x \in B\}$
- $A \times B := \{(x, y) \mid x \in A \text{ und } x \in B\}$
- $A^n := \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in A\}$
- $\bar{A} := \{x \in M \text{ und } x \notin A\}$, wobei M meist global gegeben ist.

▶ zurück

Beispiel

Seien $A = \{a, b, c, d\}$, $B = \{a, d, e\}$ und $M = \{a, b, c, d, e, f\}$.

- $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \dots, \{a, b, c, d\}\}$
- $A \cap B = \{a, d\}$
- $A \cup B = \{a, b, c, d, e\}$
- $A \times B = \{(a, a), (a, d), (a, e), (b, a), \dots, (c, e), (d, a), (d, d), (d, e)\}$
- $\bar{A} = \{e, f\}$
- $\bar{B} = \{b, c, f\}$