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

Erinnerung: Natürliches Schließen

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

Satz

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

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

Zusammenfassung der letzten LVA

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ 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 $a, b, c \in B$:
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \qquad a + (b \cdot c) = (a + b) \cdot (a + c)$$
3. Für alle $a \in B$ gilt
$$a + \sim(a) = 1 \qquad a \cdot \sim(a) = 0$$

Das Element $\sim(a)$ heißt das Komplement oder die Negation von a

Satz (Darstellungssatz von Stone)

Jede Boolesche Algebra $\mathcal{B}$ ist isomorph zu einer Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$, wobei M geeignet aus Elementen von $\mathcal{B}$ gewählt wird.

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

universität
innsbruck

Boolesche Algebren

Isomorphie

vgl. Lineare Algebra

Definition

Seien $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$, $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$ Algebren, dann heißt eine Abbildung $\varphi\colon A \to B$ ein Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$, wenn gilt

- φ ist bijektiv
- für alle Operationen $\circ_i$ von $\mathcal{A}$ ($\circ_i$ n-stellig) gilt:

$$\varphi(\circ_i(a_1, \ldots, a_n)) = \odot_i(\varphi(a_1), \ldots, \varphi(a_n)) \,,$$

für alle $a_1, \ldots, a_n \in A$.

Definition

Eine Algebra $\mathcal{A} = \langle A; \circ_1, \ldots, \circ_m \rangle$ heißt isomorph zur Algebra $\mathcal{B} = \langle B; \odot_1, \ldots, \odot_m \rangle$, wenn ein Isomorphismus $\varphi\colon A \to B$ existiert. Wir schreiben $\mathcal{A} \cong \mathcal{B}$.

Beispiel

- Betrachte die Monoide $\langle \{a, b\}, + \rangle$ und $\langle \{0, 1\}, \cdot \rangle$, wobei die Operationen $+$ bzw. $\cdot$ durch die folgenden Operationstafeln definiert sind:

$+$	a	b
a	a	b
b	b	a

$\cdot$	0	1
0	0	1
1	1	0

- Dann ist die Abbildung $\varphi \colon \{a, b\} \to \{0, 1\}$ mit

$$\varphi(a) := 0 \qquad \varphi(b) := 1 \,,$$

ein Isomorphismus

Bemerkung

Wir interessieren uns besonders für Isomorphismen zwischen Booleschen Algebren und können damit den Darstellungsatz von Stone exakt definieren.

Beispiel

- Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra
- Sei $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$ die Mengenalgebra, mit der Menge $M := \{a\}$. Wir können diese Mengenalgebra einfacher wie folgt schreiben:

$$\langle \{\varnothing, \{a\}\}; \cup, \cap, \sim, \varnothing, \{a\} \rangle$$

- Sei $\varphi \colon \mathbb{B} \to \{\varnothing, \{a\}\}$ wie folgt definiert

$$\varphi(0) := \varnothing \qquad \varphi(1) := \{a\}$$

- Dann ist φ eine bijektive Funktion und außerdem sogar ein Isomorphismus:

$\cup$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\{a\}$
$\varnothing$	$\{a\}$	$\varnothing$

$\cap$	$\{a\}$	$\varnothing$
$\{a\}$	$\{a\}$	$\varnothing$
$\varnothing$	$\varnothing$	$\varnothing$

$\sim$	
$\{a\}$	$\varnothing$
$\varnothing$	$\{a\}$

Partielle Ordnungen und Boolesche Algebren

Definition

Eine partielle Ordnung auf einer Menge $M \neq \varnothing$ ist eine Menge von geordneten Paaren $(a, b) \in M \times M$, geschrieben $a \leq b$, sodass gilt

- $a \leq a$, für alle $a \in M$ — Reflexivität
- $a \leq b$ und $b \leq c$ impliziert $a \leq c$, für alle $a, b, c \in M$ — Transitivität
- $a \leq b$ und $b \leq a$ impliziert $a = b$, für alle $a, b \in M$ — Antisymmetrie

Fakt

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine Boolesche Algebra und definiere Relation $\leq$ auf B:

$$a \leq b \Leftrightarrow a \cdot b = a$$

- $\leq$ ist eine partielle Ordnung

Beweis des Darstellungsatz von Stone (I)

- Sei $\mathcal{B} = \langle B; +, \cdot, \sim, 0, 1 \rangle$ eine (endliche) Boolesche Algebra;
- sei $\leq$, die von $\mathcal{B}$ induzierte partielle Ordnung.

Definition

- Sei $a \in B \setminus \{0\}$.
- Wenn $0 \leq a$ und kein $a' \in B \setminus \{0\}$, $a \neq a'$ existiert, sodass $0 \leq a' \leq a$, dann nennen wir a ein Atom.

Kürzer: die Atome sind die oberen Nachbarn von 0 in B.

Beispiel

Sei $\langle \mathbb{B}; +, \cdot, \sim, 0, 1 \rangle$ die binäre Algebra, dann ist $1 \in \mathbb{B}$ ein Atom. Es gibt kein Element $\neq 0$ in $\mathbb{B}$ gibt, das größer als 0 und (echt) kleiner als 1 ist.

Beweis des Darstellungsatz von Stone (II)

Lemma

Zu jedem $b \in B \setminus \{0\}$ gibt es mindestens ein Atom $a \in B$ mit $a \leq b$. ■

Konstruktion

1. Sei $M := \{a \in B \mid a \text{ ein Atom in } \mathcal{B}\}$.
2. Wir betrachten nun die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$.
3. Für jedes $b \in B$, definiere $A(b) := \{a \in B \mid a \text{ ein Atom in } \mathcal{B} \text{ und } a \leq b\}$.
4. Schließlich definieren wir die Abbildung $\varphi \colon B \to \mathcal{P}(M)$, sodass $\varphi(b) := A(b)$.

Lemma

Die Abbildung φ ist ein Isomorphismus von $\langle B; +, \cdot, \sim, 0, 1 \rangle$ auf $\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$. ■

universität
innsbruck

Formale Sprachen

Definition (Alphabet)

Ein Alphabet Σ ist eine endliche, nicht leere Menge von Symbolen

Beispiel

- $\Sigma = \{0, 1\}$ ist das binäre Alphabet
- $\Sigma = \{a, b, \ldots, z\}$, die Menge aller Kleinbuchstaben
- die Menge der (druckbaren) ASCII-Zeichen

Definition (Wort)

- Eine Zeichenreihe (ein Wort, ein String) ist eine endliche Folge von Symbolen über einem Alphabet Σ
- Die leere Zeichenreihe wird mit ϵ bezeichnet

Beispiel

Die Symbolkette 01101 ist eine Zeichenreihe über dem Alphabet $\{0, 1\}$

Konvention

- Buchstaben werden mit a, b, c, ... bezeichnet
- Wörter werden mit x, y, z, ... bezeichnet
- $\epsilon \notin \Sigma$

Definition (Wortlänge)

- Die Länge eines Wortes w ist die Anzahl der Positionen in w
- Die Länge von w wird auch mit $|w|$ bezeichnet
- Das Leerwort ϵ hat die Länge 0

Definition ($\Sigma^k, \Sigma^+, \Sigma^*$)

- Definiere Σ^k als die Menge der Wörter der Länge k, deren Symbole aus Σ stammen — Σ^k
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \cdots$ — Σ^+
- $\Sigma^* = \Sigma^+ \cup \{\epsilon\}$ — Σ^*

Beispiel

Sei $\Sigma = \{0, 1\}$. Dann ist

- $\Sigma^0 = \{\epsilon\}$
- $\Sigma^1 = \{0, 1\}$
- $\Sigma^2 = \{00, 01, 10, 11\}$
- $\Sigma^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$

Definition

Seien x, y Wörter über Σ, wir schreiben $x \cdot y$ für die Konkatenation von x und y

$$\epsilon \cdot x = x$$
$$(ax) \cdot y = a(x \cdot y)$$

Hier gilt $a \in \Sigma$.

Beispiel

- Sei $x = 01101$, $y = 110$, $z = 10101$
- Dann ist $x \cdot y = 01101110$ und $y \cdot x = 11001101$

Lemma

- *Konkatenation ist assoziativ und besitzt das Leerwort ϵ als neutrales Element*
- *Wir lassen $\cdot$ oft weg und schreiben xy statt $x \cdot y$*
- *Die Algebra $\langle \Sigma^*; \cdot, \epsilon \rangle$ ist ein Monoid; das Wortmonoid*

Formale Sprachen

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Beispiel

- Die Sprache aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$:
$$\{\epsilon, 01, 0011, 000111, \cdots\}$$
- Die Menge der Wörter, die jeweils die selbe Anzahl 0en und 1er enthalten:
$$\{\epsilon, 01, 10, 0011, 0101, \cdots\}$$
- Σ^* ist eine Sprache, $\varnothing$—die leere Sprache—ist eine Sprache, $\{\epsilon\}$ ist eine Sprache. Beachte $\{\epsilon\} \neq \varnothing$

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert
$$L \cup M = \{x \mid x \in L \text{ oder } x \in M\}$$
- Wir definieren das Komplement von L:
$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$
- Der Durchschnitt von L und M ist wie folgt definiert:
$$L \cap M = \{x \mid x \in L \text{ und } x \in M\}$$
- Das Produkt (oder Verkettung) von L und M ist definiert als:
$$LM = \{xy \mid x \in L, y \in M\}$$

Lemma

Seien L, L_1, L_2, L_3 formale Sprachen, dann gilt

$$(L_1L_2)L_3 = L_1(L_2L_3) \qquad L\{\epsilon\} = \{\epsilon\}L = L$$

Definition

Sei L eine formale Sprache und $k \in \mathbb{N}$

Die k-te Potenz von L definiert als:

$$L^k = \begin{cases} \{\epsilon\} & \text{falls } k = 0 \\ L & \text{falls } k = 1 \\ \underbrace{LL \cdots L}_{k\text{-mal}} & \text{falls } k > 1 \end{cases}$$

Definition

Der Kleene-Stern * oder Abschluss von L ist wie folgt definiert:

$$L^* = \bigcup_{k \geqslant 0} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k \geqslant 0\}$$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k > 0\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die Sprache L aller Wörter, die aus n 0en gefolgt von n 1er bestehen, wobei $n \geqslant 0$
- Wir können L konzise in Mengennotation angeben:

$$L = \{0^n 1^n \mid n \geqslant 0\}$$

- Es gilt $010101 \notin L$, aber $010011 \in L^2$
- Allgemein erhalten wir etwa:

$$L^2 = \{0^n 1^n 0^k 1^k \mid n, k \geqslant 0\}$$