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

Folgerung

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

Definition (Algebra)

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

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

Lemma

Jede binäre Operation hat maximal ein neutrales Element

Lemma

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

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

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

Konventionen

- Wir lassen $\cdot$ oft weg und schreiben ab statt $a{\cdot}b$
- Wir verwenden die folgende Präzedenz: $\sim$ bindet stärker als $+$ und $\cdot$
- Die Definition ist eine Verallgemeinerung der Definition in Rechnerarchitektur

Definition (Boolescher Ausdruck)

Sei eine unendliche Menge von Variablen $x_1, x_2, \ldots$ gegeben; diese Variablen heißen Boolesche Variablen

Wir definieren Boolesche Ausdrücke induktiv:

1. 0, 1 und Variablen sind Boolesche Ausdrücke
2. Wenn E und F Boolesche Ausdrücke sind, dann sind

$$\sim(E) \qquad (E \cdot F) \qquad (E + F)$$

Boolesche Ausdrücke A und B heißen äquivalent ($A \approx B$), wenn für alle Booleschen Algebren, in allen Instanzen A' und B' gilt: $A' = B'$.

Beispiel (vgl Rechnerarchitektur)

Die folgenden Ausdrücke sind Boolesche Ausdrücke:

$$x_1 \quad x_2 \quad x_1 + x_2 \quad x_1 \cdot x_2 \quad x_1 \cdot (x_1 + x_2) \quad x_1(x_1 + x_2) \quad x_1 \sim(x_1 + x_2)$$

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

$$\langle \mathcal{P}(M); \cup, \cap, \sim, \varnothing, M \rangle$$

1. $\cup$ die Mengenvereinigung
2. $\cap$ die Schnittmenge
3. $\sim$ die Komplementärmenge

Diese Algebra nennt man Mengenalgebra.

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Binäre Algebra

Definition

Sei $\mathbb{B} := \{0, 1\}$, wobei $0, 1 \in \mathbb{N}$. Wir betrachten die Algebra

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

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

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

$+$	1	0
1	1	1
0	1	0

$\sim$	
1	0
0	1

Diese Algebra nennt man binäre Algebra oder Boolesche Algebra im engeren Sinn (Rechnerarchitektur)

Lemma

Die binäre Algebra ist eine Boolesche Algebra

Algebra der Aussagenlogik

Sei Frm die Menge der aussagenlogischen Formeln

Definition

Wir betrachten die Algebra $\mathcal{F}rm$

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

Wobei die Zeichen wie in der Aussagenlogik interpretiert werden und Gleichheit von Booleschen Ausdrücken logische Äquivalenz bedeutet

Lemma

Die Algebra $\mathcal{F}rm$ ist eine Boolesche Algebra

Algebra des Kartesischen Produkts und der Schaltfunktionen

Definition

Sei $\mathbb{B} := \{0, 1\}$ und sei $\mathbb{B}^n$ das n-fache kartesische Produkt von $\mathbb{B}$: $\mathbb{B}^n = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{B}\}$; wir betrachten

$$\langle \mathbb{B}^n; +, \cdot, \sim, (0, \dots, 0), (1, \dots, 1) \rangle$$

1. $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$
2. $(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 \cdot b_1, \dots, a_n \cdot b_n)$
3. $\sim((a_1, \dots, a_n)) = (\sim(a_1), \dots, \sim(a_n))$

Lemma

Die oben definierte Algebra ist eine Boolesche Algebra

Definition

Sei Abb die Menge der Abbildungen von $\mathbb{B}^n$ nach $\mathbb{B}^m$ wir betrachten

$$\langle \mathrm{Abb}; +, \cdot, \sim, (\mathbf{0}, \dots, \mathbf{0}), (\mathbf{1}, \dots, \mathbf{1}) \rangle$$

1. $(\mathbf{0}, \dots, \mathbf{0}) \colon (a_1, \dots, a_n) \mapsto (0, \dots, 0)$
2. $(\mathbf{1}, \dots, \mathbf{1}) \colon (a_1, \dots, a_n) \mapsto (1, \dots, 1)$
3. $(f + g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) + g(a_1, \dots, a_n)$
4. $(f \cdot g)(a_1, \dots, a_n) = f(a_1, \dots, a_n) \cdot g(a_1, \dots, a_n)$
5. $\sim(f)(a_1, \dots, a_n) = \sim(f(a_1, \dots, a_n))$

Diese Algebra nennt man Algebra der Schaltfunktionen oder n-stelligen Booleschen Funktionen

Lemma

Die Algebra der Schaltfunktionen ist eine Boolesche Algebra

Lemma

Die Mengenalgebra ist eine Boolesche Algebra

Beweis.

Wir müssen zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind
2. seien $A, B, C \subseteq M$, dann gilt
$$A \cap (B \cup C) = (A \cap B) \cup (A \cup C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
3. für alle $A \subseteq M$ gilt
$$A \cup {\sim}(A) = M \quad A \cap {\sim}(A) = \varnothing$$

Wir beginnen mit den Gesetzen zum Komplement; dazu beschränken wir uns auf $A \cap {\sim}(A) = \varnothing$, der Beweis für $A \cup {\sim}(A) = M$ ist ganz ähnlich

$$A \cap {\sim}(A) = A \cap \{x \in M \mid x \notin A\} = \{x \in M \mid x \in A \text{ und } x \notin A\} = \varnothing$$

Beweis (Fortsetzung).

Wir müssen also noch zeigen, dass

1. $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ sowie $\langle \mathcal{P}(M); \cap, M \rangle$ kommutative Monoide sind
2. seien $A, B, C \subseteq M$, dann gilt

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Die Korrektheit der Distributivgesetze folgt leicht aus den Definitionen der Mengenoperationen (nachrechnen!)

Zeigen wir nun also, dass $\langle \mathcal{P}(M); \cup, \varnothing \rangle$ ein kommunitative Monoid ist; dazu zeigen wir

- $\cup$ ist assoziativ : $A \cup (B \cup C) = (A \cup B) \cup C$
- $\varnothing$ ist das neutrale Element für $\cup$ auf $\mathcal{P}(M)$: $A \cup \varnothing = \varnothing \cup A = A$

Beide Gleichungen folgen aus der Definition der Vereinigung.

Ebenso zeigt man, dass $\langle \mathcal{P}(M); \cap, M \rangle$ ein kommunitative Monoid ist. ∎

Gesetze Boolescher Algebren

die noch nicht in Rechnerarchitektur behandelt wurden

Lemma ①

Für alle $a, b \in B$ gilt die Eindeutigkeit des Komplements:

$$\textit{Wenn } a + b = 1 \textit{ und } ab = 0\textit{, dann } b = \sim(a)$$

Beweis.

Gelte $a + b = 1$ und $ab = 0$

$$\begin{aligned}
b &= b1 = b(a + \sim(a)) \\
&= ba + b \cdot \sim(a) = 0 + b \cdot \sim(a) && \text{da } ba = ab = 0 \\
&= a \cdot \sim(a) + b \cdot \sim(a) = (a + b) \cdot \sim(a) \\
&= 1 \cdot \sim(a) && \text{da } a + b = 1 \\
&= \sim(a)
\end{aligned}$$

Lemma

Für alle $a \in B$ gilt das Involutionsgesetz:

$$\sim(\sim(a)) = a$$

Beweis.

Nach Definition einer Booleschen Algebra und Kommutativität von $+$ beziehungsweise $\cdot$ gilt:

1. $\sim(a) + a = 1$
2. $\sim(a) \cdot a = 0$

Mit Lemma ① folgt, dass a das Komplement von $\sim(a)$ ist ∎

Lemma

Für alle $a, b \in B$ gelten die Gesetze von de Morgan:

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

Idempotenz und Absorption

bereits in Rechnerarchitektur behandelt

Lemma

Für alle $a \in B$ gelten die Idempotenzgesetze:

$$a \cdot a = a \qquad a + a = a$$

und die folgenden Gesetze für 0 und 1 (Substitution):

$$0 \cdot a = 0 \qquad 1 + a = 1$$

Lemma

Für alle $a, b \in B$ gelten die Absorptionsgesetze:

$$a + ab = a \qquad a(a + b) = a$$

$$a + \sim(a) \cdot b = a + b \qquad a(\sim(a) + b) = ab$$

Erstes Gesetz von de Morgan.

- Wir zeigen $(a + b) + (\sim(a) \cdot \sim(b)) = 1$:

$$\begin{aligned}(a + b) + (\sim(a) \cdot \sim(b)) &= (a + b + \sim(a))(a + b + \sim(b))\\ &= (a + \sim(a) + b)(a + b + \sim(b))\\ &= (1 + b)(a + 1)\\ &= 1 \cdot 1 = 1\end{aligned}$$

- Wir zeigen $(a + b) \cdot (\sim(a) \cdot \sim(b)) = 0$:

$$\begin{aligned}(a + b) \cdot \sim(a) \cdot \sim(b) &= a \cdot \sim(a) \cdot \sim(b) + b \cdot \sim(a) \cdot \sim(b)\\ &= a \cdot \sim(a) \cdot \sim(b) + \sim(a) \cdot b \cdot \sim(b)\\ &= 0 \cdot \sim(b) + \sim(a) \cdot 0\\ &= 0 + 0 = 0\end{aligned}$$

- Die Voraussetzungen von Lemma ① sind gezeigt
- Somit ist $\sim(a) \cdot \sim(b)$ das Komplement von $a + b$, wzzw. ■

Definition (Boolesche Funktion)

1. Sei F ein Boolescher Ausdruck in den Variablen $x_1, \dots, x_n$
2. $F(s_1, \dots, s_n)$ die Instanz von F
3. Wir definieren die Funktion $f \colon \mathbb{B}^n \to \mathbb{B}$ wie folgt:

$$f(s_1, \dots, s_n) := F(s_1, \dots, s_n) \ .$$

Dann heißt f die Boolesche Funktion zum Ausdruck F

Beispiel (Boolesche Algebra $\mathcal{F}rm = \langle \mathsf{Frm}; \vee, \wedge, \neg, \mathsf{False}, \mathsf{True} \rangle$)

Sei $F = x_1 \wedge \neg(x_2 \vee x_1)$, dann ist $f \colon \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zu F

Sei $G = x_1 \wedge x_2 \wedge \neg x_2$, dann ist $g \colon \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zu G

s_1	s_2	$f(s_1, s_2)$	$g(s_1, s_2)$
0	0	0	0
0	1	0	0
1	0	0	0
1	1	0	0

Definition

1. Sei $f \colon \mathbb{B}^n \to \mathbb{B}$ eine Boolesche Funktion
2. Sei F ein Boolescher Ausdruck, dessen Boolesche Funktion gleich f

Dann nennen wir F den Booleschen Ausdruck von f

Satz (Darstellungssatz von Stone)

Jede Boolesche Algebra ist isomorph zu einer Mengenalgebra

Bemerkung

- Isomorphie bedeutet, dass die Operationen auf den Algebren ident sind.
- Der Darstellungssatz von Stone bedeutet also, dass jede Gleichheit in einer Mengenalgebra eine Gleichheit für alle Booleschen Algebren ist.
- Anders ausgedrückt stellen Mengenalgebren die eindeutige Darstellung von Booleschen Algebren dar.

Folgerung aus dem Darstellungssatz von Stone

Folgerung

1. *Seien A, B Boolesche Ausdrücke*
2. *Seien f, g ihre Booleschen Funktionen*

Dann sind A und B äquivalent ($A \approx B$), wenn $f = g$ in der Algebra der Booleschen Funktionen gilt

Beweisskizze

- Äquivalenzen von Boolesche Ausdrücke gelten (per Definition) für alle Booleschen Algebren.
- Um diese Äquivalenzen zu überprüfen genügt (nach der Definition) die Verifikation in einer bestimmten Algebra, nämlich der Algebra der Booleschen Funktionen; das folgt aus dem Darstellungssatz von Stone