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

Lemma

Jede binäre Operation hat maximal ein neutrales Element und wenn $\mathcal{A} = \langle A; \circ, 1\rangle$ ein Monoid ist, dann ist das Inverse eindeutig

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

Definition

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

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

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

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

Lemma

Die Algebra der Schaltfunktionen ist eine Boolesche Algebra

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

Gesetze Boolescher Algebren

die noch nicht in Rechnerarchitektur behandelt wurden

Lemma ①

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

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

Beweis.

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

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

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:

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

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 $a + b$ ■

Definition (Boolesche Funktion)

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

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

Dann heißt f die Boolesche Funktion zum Ausdruck F

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

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

Satz

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

Dann gilt $A \approx B$ gdw. $f = g$ in der Algebra der Booleschen Funktionen

Universelle Algebra

Definition (Signatur)

- Eine Signatur F ist eine Menge von Funktionssymbolen (Symbolen für Operationen)
- Jedem $f \in \mathrm{F}$ ist eine Stelligkeit n zugeordnet
- Symbole mit Stelligkeit 0 werden Konstanten genannt

Sei F eine Signatur und sei V eine (unendliche) Menge von Variablen

Definition (Terme)

Die Menge $\mathrm{T}(\mathrm{F}, \mathrm{V})$ aller Terme (über F) ist induktiv definiert:

1. Jedes Element von V ist ein Term
2. Wenn $f \in \mathrm{F}$ mit Stelligkeit n sowie $t_1, \ldots, t_n$ Terme, dann ist auch $f(t_1, \ldots, t_n)$ ein Term

Definition (Substitution)

- Eine Substitution ist eine Abbildung $\sigma\colon \mathrm{V} \to \mathrm{T}(\mathrm{F}, \mathrm{V})$
- $\{x \in \mathrm{V} \mid \sigma(x) \neq x\}$ ist Definitionsbereich $\mathrm{dom}(\sigma)$ von σ
- Wenn $\mathrm{dom}(\sigma) = \{x_1, \ldots, x_n\}$ können wir schreiben:

$$\sigma = \{x_1 \mapsto \sigma(x_1), \ldots, x_n \mapsto \sigma(x_n)\}$$

- Wir definieren den Wertebereich von σ

$$\mathrm{range}(\sigma) = \{\sigma(x) \mid x \in \mathrm{dom}(\sigma)\}$$

Beispiel

Sei $\mathrm{F} = \{\sim, \cdot, +, 0, 1\}$ eine Signatur und sei $\mathrm{V} = \{x_1, x_2, \ldots\}$; betrachte

$$x_1 \quad x_2 \quad \sim(x_3) \quad x_4 \quad x_1 \cdot x_2 \quad x_2 \cdot (x_3 + x_4) \quad x_1 \cdot \sim((x_3 + x_4))$$

$$\sigma = \{x_1 \mapsto x_2, x_2 \mapsto x_3 + x_4\} \qquad (x_1 \cdot x_2)\sigma = x_2 \cdot (x_3 + x_4)$$

Gleichungen und Gleichungslogik

Definition

Substitution σ kann zur Abbildung $\overline{\sigma}\colon \mathsf{T}(\mathsf{F},\mathsf{V}) \to \mathsf{T}(\mathsf{F},\mathsf{V})$ erweitert werden:

$$\overline{\sigma}(t) := \begin{cases} \sigma(t) & \text{wenn } t \in \mathsf{V} \\ f(\overline{\sigma}(t_1),\ldots,\overline{\sigma}(t_n)) & \text{wenn } t = f(t_1,\ldots,t_n) \end{cases}$$

Fakt

Die Anwendung (der Erweiterung) einer Substitution auf einen Term ersetzt simultan alle Variablen im Definitionsbereich durch ihr Bild.

Konvention

Wir bezeichnen die Erweiterung $\overline{\sigma}$ einer Substitution σ, wiederum mit σ

Definition (Gleichung)

Eine Gleichung über der Signatur F ist ein Paar $s \approx t$ von Termen

Sei E eine Menge von Gleichungen (oder Identitäten)

Definition (Gleichungslogik)

$$[\mathrm{r}]\ \frac{}{E \vdash t \approx t} \qquad [\mathrm{s}]\ \frac{E \vdash s \approx t}{E \vdash t \approx s}$$

$$[\mathrm{t}]\ \frac{E \vdash s \approx t \quad E \vdash t \approx u}{E \vdash s \approx u} \qquad [\mathrm{a}]\ \frac{s \approx t \in E}{E \vdash s \approx t}$$

$$[\mathrm{i}]\ \frac{E \vdash s \approx t}{E \vdash \sigma(s) \approx \sigma(t)}\ \sigma \text{ eine Substitution}$$

$$[\mathrm{k}]\ \frac{E \vdash s_1 \approx t_1 \quad \ldots \quad E \vdash s_n \approx t_n}{E \vdash f(s_1,\ldots,s_n) \approx f(t_1,\ldots,t_n)}$$

Beispiele

1. Wir betrachten die Signatur
$$\mathsf{F} = \{+, \mathsf{s}, 0\}$$
Stelligkeit von 0 ist 0, Stelligkeit von s ist 1, Stelligkeit von $+$ ist 2 und wir schreiben $+$ oft in Infix
2. Wir betrachten die Menge von Variablen $\mathsf{V} = \{x, y\}$
3. Die folgenden Ausdrücke sind Terme in $\mathsf{T}(\mathsf{F},\mathsf{V})$
$$x \qquad +(x,y) \qquad +(\mathsf{s}(x),y) \qquad 0{+}\mathsf{s}(y)$$
4. Wir betrachten das Paar von Termen $(\mathsf{s}(\mathsf{s}(0)+\mathsf{s}(0)), \mathsf{s}(\mathsf{s}(\mathsf{s}(0))))$ und schreiben dieses:
$$\mathsf{s}(\mathsf{s}(0)+\mathsf{s}(0)) \approx \mathsf{s}(\mathsf{s}(\mathsf{s}(0))) \qquad (1)$$
Dann ist (1) eine Gleichung

Beispiel

Wir betrachten die Abbildung $\sigma\colon \mathsf{V} \to \mathsf{T}(\mathsf{F},\mathsf{V})$

$$\sigma(z) = \begin{cases} x{+}y & z = x \\ z & \text{sonst} \end{cases}$$

Die Funktion σ ist eine Substitution mit Wertebereich $\mathrm{dom}(\sigma) = \{x\}$

Beispiel

Wir betrachten die Menge der Identitäten E

$$0{+}x \approx x \qquad \mathsf{s}(x){+}y \approx \mathsf{s}(x{+}y)$$

Dann gilt $E \vdash \mathsf{s}(\mathsf{s}(0)+\mathsf{s}(0)) \approx \mathsf{s}(\mathsf{s}(\mathsf{s}(0)))$

Gleichungen für Boolesche Ausdrücke

Beispiel

1. Wir betrachten die folgende Signatur

$$\mathsf{F} = \{\sim, +, 0, 1\}$$

   sodass
   - Stelligkeit von 0, 1 ist 0
   - Stelligkeit von $\sim$ ist 1
   - Stelligkeit von $+$ ist 2

2. $\mathsf{V} = \{x_1, x_2, \dots\}$
3. Wir betrachten die Identitäten E

$$(x+y)+z \approx x+(y+z) \quad \sim(x)+x \approx 1 \quad x+x \approx x$$

4. Dann gilt $E \vdash 1+x \approx 1$

Beispiel (Fortsetzung)

Zunächst betrachten wir die folgende „Herleitung“ der Gleichung:

$$1+x \approx (\sim(x)+x)+x \approx \sim(x)+(x+x) \approx \sim(x)+x \approx 1$$

Formal in der Gleichungslogik:

$$\frac{E \vdash 1+x \overset{①}{\approx} (\sim(x)+x)+x \quad E \vdash (\sim(x)+\overset{②}{x})+x \approx 1}{E \vdash 1+x \approx 1}\ [\mathrm{t}]$$

Wir betrachten ①:

$$\dfrac{\dfrac{\dfrac{\sim(x)+x \approx 1 \in E}{E \vdash \sim(x)+x \approx 1}\ [\mathrm{a}]}{E \vdash 1 \approx \sim(x)+x}\ [\mathrm{s}] \quad \dfrac{}{E \vdash x \approx x}\ [\mathrm{r}]}{E \vdash 1+x \approx (\sim(x)+x)+x}\ [\mathrm{k}]$$

Beispiel (Fortsetzung)

Wir skizzieren ②:

$$\frac{E \vdash (\sim(x)+x)+\overset{③}{x} \approx \sim(x)+(x+x) \quad E \vdash \sim(x)+\overset{④}{(x+x)} \approx 1}{E \vdash (\sim(x)+x)+x \approx 1}\ [\mathrm{t}]$$