Computational Logic

Einführung in die Theoretische Informatik

Woche 5

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015

Lemma

Für jede Menge M ist die Mengenalgebra $\langle \mathcal{P}(M); \cup, \cap, \overline{\ }, \varnothing, M\rangle$ eine Boolesche Algebra.

Lemma

Die binäre Algebra $\langle \mathbb{B}; +, \cdot, \overline{\ }, 0, 1\rangle$ ist eine Boolesche Algebra.

$+$	1	0
1	1	1
0	1	0

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

$\overline{\ }$	
1	0
0	1

Lemma

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

Zusammenfassung der letzten LV

Lemma

Jede binäre Operation hat maximal ein neutrales Element. In einem Monoid ist das Inverse eines Elements eindeutig (wenn es existiert).

Definition (Boolesche Algebra)

Eine Algebra $\mathcal{B} = \langle B; +, \cdot, \overline{\ }, 0, 1\rangle$ 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

$$a + \overline{a} = 1 \qquad a \cdot \overline{a} = 0$$

Das Element $\overline{a}$ heißt das Komplement oder die Negation von a

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

Beispiele Boolescher Algebren

Definition

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

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

1. $(a_1,\ldots,a_n) + (b_1,\ldots,b_n) = (a_1+b_1,\ldots,a_n+b_n)$
2. $(a_1,\ldots,a_n) \cdot (b_1,\ldots,b_n) = (a_1\cdot b_1,\ldots,a_n\cdot b_n)$
3. $\overline{(a_1,\ldots,a_n)} = (\overline{a_1},\ldots,\overline{a_n})$

wobei $+\colon \mathbb{B}\times\mathbb{B}\to\mathbb{B}$, $\cdot\colon \mathbb{B}\times\mathbb{B}\to\mathbb{B}$ und ${}^{-}\colon \mathbb{B}\to\mathbb{B}$ wie in der binären Algebra

Lemma

Für jedes $n \in \mathbb{N}$ ist die oben definierte Algebra ist eine Boolesche Algebra.

Algebra der Booleschen Funktionen

Definition

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

$$\langle \mathrm{Abb}; +, \cdot, {}^{-}, (\mathbf{0},\ldots,\mathbf{0}), (\mathbf{1},\ldots,\mathbf{1})\rangle$$

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. $\overline{f}(a_1,\ldots,a_n) = \overline{f(a_1,\ldots,a_n)}$

Diese Algebra nennt man Algebra der n-stelligen Booleschen Funktionen

Lemma

Die Algebra der n-stelligen Booleschen Funktionen ist eine Boolesche Algebra.

Gesetze Boolescher Algebren

Lemma (Dualitätsprinzip)

1. *Sei $\mathcal{B}$ eine Boolesche Algebra*
2. *Für Boolesche Ausdrücke E und F gelte $E \approx F$ in $\mathcal{B}$*

Dann gilt eine entsprechende Gleichheit $E' \approx F'$ in $\mathcal{B}$ bei der alle Vorkommnisse von $+$ durch $\cdot$ (und umgekehrt) ersetzt sowie 0 und 1 vertauscht werden.

Im Folgenden sei $\mathcal{B} = \langle B; +, \cdot, {}^{-}, 0, 1\rangle$ eine Boolesche Algebra.

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:

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

Lemma

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

$$a + ab = a \qquad a(a+b) = a$$
$$a + \overline{a}b = a + b \qquad a(\overline{a}+b) = ab$$

Lemma ①

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

Wenn $a + b = 1$ und $ab = 0$, dann $b = \overline{a}$

Beweis.

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

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

Lemma

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

$$\overline{\overline{a}} = a$$

Beweis.

Nach Definition einer Booleschen Algebra ist

1. $a + \overline{a} = 1$ und $a \cdot \overline{a} = 0$ ($\overline{a}$ ist Komplement von a)
2. $\overline{a} + \overline{\overline{a}} = 1$ und $\overline{a} \cdot \overline{\overline{a}} = 0$ ($\overline{\overline{a}}$ ist Komplement von $\overline{a}$)

Da $+$ und $\cdot$ kommutativ folgt aus 1, dass

3. $\overline{a} + a = 1$ und $\overline{a} \cdot a = 0$ (a ist Komplement von $\overline{a}$)

Nun folgt aus 2, 3 und Lemma ①, dass $\overline{\overline{a}} = a$. ■

Lemma

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

$$\overline{a + b} = \overline{a} \cdot \overline{b} \qquad \overline{a \cdot b} = \overline{a} + \overline{b}$$

Beweis (der Gesetze von de Morgan)

- Wir zeigen $(a + b) + \overline{a} \cdot \overline{b} = 1$:

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

- Wir zeigen $(a + b) \cdot \overline{a} \cdot \overline{b} = 0$:

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

- Die Voraussetzungen von Lemma ① sind gezeigt
- Somit ist $\overline{a} \cdot \overline{b}$ das Komplement von $a + b$ ■

Sei $\mathbb{B} = \{0, 1\}$ und sei $\mathbb{B}^n$ das n-fache kartesische Produkt von $\mathbb{B}$

Definition (Boolesche Funktion)

1. Sei F ein Boolescher Ausdruck in den Variablen $x_1, \ldots, x_n$ und
2. $F(s_1, \ldots, s_n)$ die Instanz von F, die x_i durch s_i ersetzt
3. Wir definieren die Funktion $f : \mathbb{B}^n \to \mathbb{B}$ 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 $f : \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zum Ausdruck F.

Sei $G = x_1 \wedge x_2 \wedge \neg x_2$. Dann ist $g : \mathbb{B}^2 \to \mathbb{B}$ die Boolesche Funktion zum Ausdruck 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 $f : \mathbb{B}^n \to \mathbb{B}$ 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 F, G Boolesche Ausdrücke*
2. *Seien f, g ihre Booleschen Funktionen*

Dann gilt $F \approx G$ gdw. $f = g$ in der Algebra der n-stelligen Booleschen Funktionen.

Definition (Konjunktive und Disjunktive Normalformen)

1. Ein Literal ist eine Boolesche Variable x oder ihre Negation $\overline{x}$
2. Ein Summenterm ist ein Boolescher Ausdruck der Gestalt
$$l_1 + \cdots + l_n$$
wobei l_i Literale
3. Ein Produktterm ist ein Boolescher Ausdruck der Gestalt
$$l_1 \cdot \ldots \cdot l_n$$
wobei l_i Literale
4. Boolescher Ausdruck F ist in konjunktiver Normalform (KNF), wenn F das Produkt von Summentermen
5. Boolescher Ausdruck F ist in disjunktiver Normalform (DNF), wenn F die Summe von Produkttermen

Satz

Jeder Boolesche Ausdruck hat eine konjunktive beziehungsweise eine disjunktive Normalform

Universelle Algebra

Definition (Signatur)

- Eine Signatur F ist eine Menge von Funktionssymbolen (Symbolen für Operationen)
- Jedem $f \in \mathsf{F}$ 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 $\mathsf{T}(\mathsf{F},\mathsf{V})$ aller Terme (über F) ist induktiv definiert:

1. Jedes Element von V ist ein Term
2. Wenn $f \in \mathsf{F}$ mit Stelligkeit n sowie $t_1, \ldots, t_n$ Terme, dann ist auch $f(t_1, \ldots, t_n)$ ein Term (beachte Spezialfall: $n = 0$) ▸ Beispiel

Substitutionen

Definition (Substitution)

- Eine Substitution ist eine Abbildung $\sigma\colon \mathsf{V} \to \mathsf{T}(\mathsf{F},\mathsf{V})$
- Wir schreiben σ oft als Menge $\{x \mapsto \sigma(x) \mid x \in \mathsf{V}, x \neq \sigma(x)\}$

Definition

Erweiterung einer Substitution σ auf Terme $\overline{\sigma}\colon\ \mathsf{T}(\mathsf{F},\mathsf{V}) \to \mathsf{T}(\mathsf{F},\mathsf{V})$ mit

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

Beispiel

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

$x_1 \quad x_2 \quad \overline{x_3} \quad x_4 \quad x_1 \cdot x_2 \quad x_2 \cdot (x_3 + x_4) \quad x_1 \cdot \overline{(x_3 + x_4)}$ ▸ zurück

$\sigma = \{x_1 \mapsto x_2, x_2 \mapsto x_3 + x_4\}$

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

Substitutionen (2) und Gleichungen

Fakt

Die Anwendung (der Erweiterung) einer Substitution σ auf einen Term ersetzt simultan alle Variablen x durch ihr Bild $\sigma(x)$.

Konvention

Im Folgenden bezeichnen wir die Erweiterung $\overline{\sigma}$ einer Substitution σ, wiederum mit σ.

Definition (Gleichung)

Eine Gleichung (über der Signatur F) ist ein Paar (s, t) von Termen (über F).
Wir schreiben $s \approx t$ für Gleichungen. Verwechslungsgefahr mit Äquivalenz!

Gleichungslogik

Sei E eine Menge von Gleichungen

Definition (Gleichungslogik)

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

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

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

Definition

Wir schreiben $E \vdash s \approx t$, wenn $s \approx t$ syntaktisch aus E folgt, dh. es einen Beweis in der Gleichungslogik gibt.

Beispiele zur Universellen Algebra

Beispiele

1. Wir betrachten die Signatur $\mathrm{F} = \{+, \mathrm{s}, 0\}$. Stelligkeit von 0 ist 0, Stelligkeit von s ist 1, Stelligkeit von $+$ ist 2 (wir schreiben $+$ oft infix)
2. Wir betrachten die Menge von Variablen $\mathrm{V} = \{x, y, \ldots\}$
3. Die folgenden Ausdrücke sind Terme in $\mathrm{T}(\mathrm{F}, \mathrm{V})$

   $$x \quad +(x, y) \quad +(\mathrm{s}(x), y) \quad 0 + \mathrm{s}(y) \quad \mathrm{s}(0) + \mathrm{s}(0)) \quad \mathrm{s}(\mathrm{s}(0)))$$

4. Dann ist $\mathrm{s}(\mathrm{s}(0) + \mathrm{s}(0)) \approx \mathrm{s}(\mathrm{s}(0)))$ eine Gleichung.
5. Wir betrachten die Substitution $\sigma \colon \mathrm{V} \to \mathrm{T}(\mathrm{F}, \mathrm{V})$

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

   Wir schreiben σ als $\{x \mapsto x + y\}$.

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

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

Beispiel

Wir betrachten die Menge der Gleichungen E

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

Dann gilt $E \vdash \mathrm{s}(\mathrm{s}(0) + \mathrm{s}(0)) \approx \mathrm{s}(\mathrm{s}(0)))$, da

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathrm{s}(x) + y \approx \mathrm{s}(x + y) \in E}{E \vdash \mathrm{s}(x) + y \approx \mathrm{s}(x + y)}\,[\mathrm{a}]}{E \vdash \mathrm{s}(0) + \mathrm{s}(0) \approx \mathrm{s}(0 + \mathrm{s}(0))}\,[\mathrm{i}],\ \sigma_1 \quad \dfrac{\dfrac{0 + x \approx x \in E}{E \vdash 0 + x \approx x}\,[\mathrm{a}]}{E \vdash 0 + \mathrm{s}(0) \approx \mathrm{s}(0)}\,[\mathrm{i}],\ \sigma_2}{E \vdash \mathrm{s}(0 + \mathrm{s}(0)) \approx \mathrm{s}(\mathrm{s}(0))}\,[\mathrm{k}]}{E \vdash \mathrm{s}(0) + \mathrm{s}(0) \approx \mathrm{s}(\mathrm{s}(0)))}\,[\mathrm{t}]}{E \vdash \mathrm{s}(\mathrm{s}(0) + \mathrm{s}(0)) \approx \mathrm{s}(\mathrm{s}(0)))}\,[\mathrm{k}]$$

Hier verwenden wir $\sigma_1 = \{x \mapsto 0, y \mapsto \mathrm{s}(0)\}$ und $\sigma_2 = \{x \mapsto \mathrm{s}(0)\}$.