Einführung in die Theoretische Informatik

Woche 6

Harald Zankl

Institut für Informatik @ UIBK

Wintersemester 2014/2015

Zusammenfassung der letzten LV

Satz

1. *Seien F, G Boolesche Ausdrücke (in den Variablen $x_1, \dots, x_n$)*
2. *Seien $f\colon \mathbb{B}^n \to \mathbb{B}$, $g\colon \mathbb{B}^n \to \mathbb{B}$ ihre Booleschen Funktionen*

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

Folgerung

- *Äquivalenzen von Booleschen Ausdrücken gelten (per Definition) für alle Booleschen Algebren*
- *Um diese Äquivalenzen zu überprüfen genügt (nach obigem Satz) der Test in der Algebra der n-stelligen Booleschen Funktionen*

Definition (Gleichung)

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

Sei E eine Menge von Gleichungen

Definition (Gleichungslogik)

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

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

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

Frage

Wie zeigt man $E \nvdash s \approx t$?

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

Gleichungen für Boolesche Ausdrücke

Beispiel

1. Wir betrachten die folgende Signatur

$$\mathrm{F} = \{+, \cdot, {}^{-}, 0, 1\}$$

   sodass
   - Stelligkeit von 0, 1 ist 0
   - Stelligkeit von ${}^{-}$ ist 1
   - Stelligkeit von $+$, $\cdot$ ist 2
2. $\mathrm{V} = \{x, y, \dots\}$
3. Wir betrachten die Gleichungen E

$$(x+y)+z \approx x+(y+z) \qquad \overline{x}+x \approx 1 \qquad x+x \approx x$$

4. Dann gilt $E \vdash 1+x \approx 1$ (nächste Folie)
5. Dann gilt $E \nvdash x+1 \approx 1$ (diese Vorlesung)

Beispiel (Fortsetzung)

Zunächst betrachten wir die folgende „Herleitung“ der Gleichung:

$$1+x \approx (\overline{x}+x)+x \approx \overline{x}+(x+x) \approx \overline{x}+x \approx 1$$

Formal in der Gleichungslogik:

$$\dfrac{\overset{\text{①}}{E \vdash 1+x \approx (\overline{x}+x)+x} \qquad \overset{\text{②}}{E \vdash (\overline{x}+x)+x \approx 1}}{E \vdash 1+x \approx 1}\,[\mathrm{t}]$$

Wir betrachten ①:

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

Wir skizzieren ②:

$$\dfrac{\begin{array}{c}\vdots\\ E \vdash (\overline{x}+x)+x \approx \overline{x}+(x+x)\end{array} \qquad \begin{array}{c}\vdots\\ E \vdash \overline{x}+(x+x) \approx 1\end{array}}{E \vdash (\overline{x}+x)+x \approx 1}\,[\mathrm{t}]$$

Vollständigkeit und Korrektheit der Gleichungslogik

Frage

1. Ist die Gleichungslogik korrekt?

   Sind (zum Beispiel) alle Schlussfolgerungen aus den Gesetzen der Booleschen Algebra wirklich Äquivalenzen von Booleschen Ausdrücken?
2. Ist die Gleichungslogik vollständig?

   Kann (zum Beispiel) jede Äquivalenz von Booleschen Ausdrücken mit dem Kalkül der Gleichungslogik hergeleitet werden?

Satz (Satz von Birkhoff)

Für beliebige Terme s, t gilt $E \models s \approx t$ gdw. $E \vdash s \approx t$.

Folgerung

Die Gleichungslogik ist vollständig und korrekt.

Semantische Konsequenz

Definition

Eine Algebra $\mathcal{A}$ über der Signatur F setzt sich zusammen aus:

1. Einer Trägermenge A und
2. einer Abbildung, die jedem Funktionssymbol $f \in \mathrm{F}$ mit Stelligkeit n eine Funktion $f^{\mathcal{A}} \colon A^n \to A$ zuordnet.

Beispiel

Signatur $\mathrm{F} = \{+, {}^{-}, 1\}$. Algebra $\mathcal{A} = \langle \{0,1\}, +^{\mathcal{A}}, {}^{-\mathcal{A}}, 1^{\mathcal{A}} \rangle$ über F mit

$+^{\mathcal{A}}$	0	1
0	0	1
1	1	1

${}^{-\mathcal{A}}$	
0	1
1	1

$1^{\mathcal{A}}$	
	1

Bemerkung

eine Algebra $\mathcal{A}$ über einer Signatur ist eine Algebra

Semantische Konsequenz (cont'd)

Definition

- Sei $\mathcal{A}$ eine Algebra (über der Signatur F)
- Sei $s \approx t$ eine Gleichung (über der Signatur F). Sind s und t äquivalent in der Algebra $\mathcal{A}$ (siehe Woche 4), schreiben wir $\mathcal{A} \models s \approx t$.

Beispiel

Sei $\mathcal{A} = \langle \{0,1\}, +^{\mathcal{A}}, -^{\mathcal{A}}, 1^{\mathcal{A}} \rangle$ eine Algebra mit

$+^{\mathcal{A}}$	0	1
0	0	1
1	1	1

$-^{\mathcal{A}}$	
0	1
1	1

$1^{\mathcal{A}}$	
	1

Dann gilt $\mathcal{A} \models (x+y)+z \approx x+(y+z)$, $\mathcal{A} \models \overline{x}+x \approx 1$, $\mathcal{A} \models x+x \approx x$.

Semantische Konsequenz (cont'd)

Definition

- Sei $\mathcal{A}$ eine Algebra (über der Signatur F)
- Sei $s \approx t$ eine Gleichung (über der Signatur F). Sind s und t äquivalent in der Algebra $\mathcal{A}$ (siehe Woche 4), schreiben wir $\mathcal{A} \models s \approx t$.

Beispiel

Sei $\mathcal{B} = \langle \{0,1\}, +^{\mathcal{B}}, -^{\mathcal{B}}, 1^{\mathcal{B}} \rangle$ eine Algebra mit

$+^{\mathcal{B}}$	0	1
0	0	0
1	1	1

$-^{\mathcal{B}}$	
0	1
1	1

$1^{\mathcal{B}}$	
	1

Dann gilt $\mathcal{B} \models (x+y)+z \approx x+(y+z)$, $\mathcal{B} \models \overline{x}+x \approx 1$, $\mathcal{B} \models x+x \approx x$.

Semantische Konsequenz (cont'd)

Definition

- Sei $\mathcal{A}$ eine Algebra (über der Signatur F)
- Sei $s \approx t$ eine Gleichung (über der Signatur F). Sind s und t äquivalent in der Algebra $\mathcal{A}$ (siehe Woche 4), schreiben wir $\mathcal{A} \models s \approx t$.

Beispiel

Sei $\mathcal{C} = \langle \{0,1\}, +^{\mathcal{C}}, -^{\mathcal{C}}, 1^{\mathcal{C}} \rangle$ eine Algebra mit

$+^{\mathcal{C}}$	0	1
0	0	0
1	1	1

$-^{\mathcal{C}}$	
0	1
1	0

$1^{\mathcal{C}}$	
	1

Dann gilt $\mathcal{C} \models (x+y)+z \approx x+(y+z)$, $\mathcal{C} \not\models \overline{x}+x \approx 1$, $\mathcal{C} \models x+x \approx x$.

Semantische Konsequenz (cont'd)

Definition

Sei E eine Menge von Gleichungen (über der Signatur F)

- Eine Algebra $\mathcal{A}$ heißt Modell von E, wenn $\mathcal{A} \models s \approx t$ für jede Gleichung $s \approx t \in E$
- Gleichung $s \approx t$ ist semantische Konsequenz von E $\quad E \models s \approx t$
  wenn folgende Implikation gilt:
  Wenn $\mathcal{A}$ Modell von E, dann $\mathcal{A} \models s \approx t$.
- Die Frage ob $E \models s \approx t$ heißt auch das Wortproblem

Beispiel (Fortsetzung)

Sei E die Menge an Gleichungen:

$$(x+y)+z \approx x+(y+z) \qquad \overline{x}+x \approx 1 \qquad x+x \approx x$$

- $\mathcal{A}$ ist Modell von E • $\mathcal{B}$ ist Modell von E • $\mathcal{C}$ ist nicht Modell von E
- $E \not\models x+1 \approx 1$ (da $\mathcal{B}$ Modell von E, aber $\mathcal{B} \not\models x+1 \approx 1$)

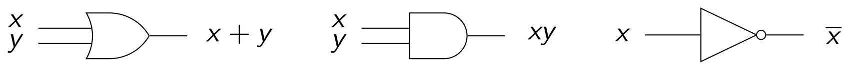
Logische Schaltkreise oder Schaltnetze

Definition

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

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

wobei die Operationen $+$, $\cdot$, $^{-}$ wie folgt definiert sind:



Diese Algebra ist eine Boolesche Algebra und heißt Schaltalgebra.

Definition

- Ein logischer Schaltkreis (Schaltnetz) ist ein algebraischer Ausdruck der Schaltalgebra
- Die Operationen $+$, $\cdot$, $^{-}$ werden mit logischen Gattern ausgedrückt

Schaltfunktionen

Definition

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

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

1. $(\mathbf{0}, \dots, \mathbf{0})$ und $(\mathbf{1}, \dots, \mathbf{1})$ sind konstante Funktionen
2. $+$, $\cdot$, $^{-}$ sind punktweise definiert

Diese Algebra nennt man Algebra der n-stelligen Schaltfunktionen

Satz

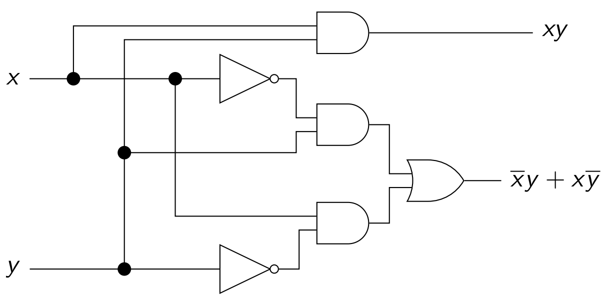
1. *Seien A, B logische Schaltkreise (in den Variablen $x_1, \dots, x_n$)*
2. *Seien $f : \mathbb{B}^n \to \mathbb{B}$, $g : \mathbb{B}^n \to \mathbb{B}$ ihre Schaltfunktionen*

Dann gilt $A \approx B$ in der Schaltalgebra gdw. $f = g$ in der Algebra der n-stelligen Schaltfunktionen.

Vereinfachen von Schaltnetzen (Halbaddierer)

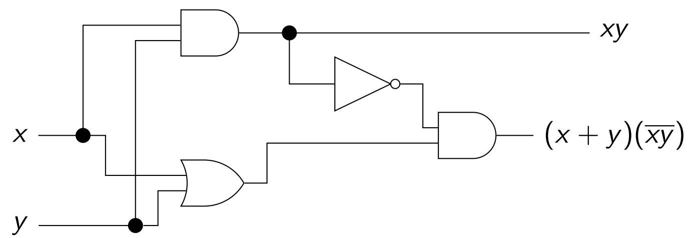
Beispiel

- Der Übertrag $\text{carry}(a, b) = 1$ gdw. $a = 1$ und $b = 1$; also $\text{carry}(a, b) = ab$
- Der Summand $\text{summand}(a, b) = 1$ gdw. $a = 0$ und $b = 1$ gilt oder $a = 1$ und $b = 0$; also $\text{summand}(a, b) = \bar{a}b + a\bar{b}$



Beispiel (cont'd)

$$\begin{aligned}
\bar{a}b + a\bar{b} &= (\bar{a}b + a)(\bar{a}b + \bar{b}) && \text{Distributivgesetz} \\
&= (a + \bar{a}b)(\bar{b} + b\bar{a}) && +, \cdot \text{ kommutativ} \\
&= (a + \bar{a}b)(\bar{b} + \bar{\bar{b}}\bar{a}) && \text{Involutionsgesetz} \\
&= (a + b)(\bar{b} + \bar{a}) && \text{Absorptionsgesetz (2x)} \\
&= (a + b)(\bar{a} + \bar{b}) && + \text{ kommutativ} \\
&= (a + b)\overline{ab} && \text{Gesetz von de Morgan}
\end{aligned}$$



Definition (Minimale DNF)

- Eine minimale DNF D eines Booleschen Ausdruckes A ist eine DNF von A mit minimaler Anzahl von Konjunktionen
- Wenn zwei DNFs von A die gleiche Anzahl von Konjunktionen haben, ist die DNF mit minimaler Anzahl von Literalen minimal

Definition (Minimale KNF)

- Eine minimale KNF K eines Booleschen Ausdruckes A ist eine KNF von A mit minimaler Anzahl von Disjunktionen
- Wenn zwei KNFs von A die gleiche Anzahl von Disjunktionen haben, ist die KNF mit minimaler Anzahl von Literalen minimal

Folgerung

Jeder Boolesche Ausdruck hat eine äquivalente minimale DNF bzw. äquivalente minimale KNF

Alphabete und Wörter

Definition (Alphabet)

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

Beispiel

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

Definition (Wort)

- Ein Wort (eine Zeichenreihe, ein String) ist eine endliche Folge von Symbolen über einem Alphabet Σ
- Das Leerwort wird mit ϵ bezeichnet

Wörter und Wortlänge

Beispiel

Die Symbolkette 01101 ist ein Wort über dem Alphabet $\{0, 1\}$

Konvention

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

Definition (Wortlänge)

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

Σ^k, Σ^+, Σ^*

Definition

- 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

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

Konkatenation

Definition

Seien x, y Wörter.
Wir schreiben $x \cdot y$ (oft auch xy) für die Konkatenation von x und y.
Sei $x = a_1 a_2 \cdots a_m$, $y = b_1 b_2 \cdots b_n$, dann ist

$$x \cdot y = a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n$$

Beispiel

- Seien $x = 01101$ und $y = 110$
- Dann ist $x \cdot y = 01101110$ und $y \cdot x = 11001101$

Lemma

- *Die Konkatenation ist assoziativ*
- *Das Leerwort ϵ ist ein neutrales Element für die Konkatenation*
- *Die Algebra $\langle \Sigma^*; \cdot, \epsilon \rangle$ ist ein Monoid (genannt: Wortmonoid)*