



Einführung in die Theoretische Informatik

David Drexel Alexander Maringele
Julian Fodor David Obwaller
Alexander Lochmann Jonas Schöpf

Georg Moser

cbr.uibk.ac.at

Zusammenfassung

Zusammenfassung der letzten LVA

Definition

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

Sei E eine Menge von Gleichungen (oder **Identitäten**)

Definition (Gleichungslogik)

$[r] \frac{}{E \vdash t \approx t}$ $[t] \frac{E \vdash s \approx t \quad E \vdash t \approx u}{E \vdash s \approx u}$ $[i] \frac{E \vdash s \approx t}{E \vdash \sigma(s) \approx \sigma(t)} \quad \sigma \text{ eine Substitution}$ $[k] \frac{E \vdash s_1 \approx t_1 \quad \dots \quad E \vdash s_n \approx t_n}{E \vdash f(s_1, \dots, s_n) \approx f(t_1, \dots, t_n)}$	$[s] \frac{E \vdash s \approx t}{E \vdash t \approx s}$ $[a] \frac{s \approx t \in E}{E \vdash s \approx t}$
--	--

Beispiel (Wiederholung)

Wir betrachten die Menge der **Identitäten E**

$$0+x \approx x \quad s(x)+y \approx s(x+y)$$

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

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

Hier verwenden wir:

- $\sigma_1 := \{x \mapsto 0, y \mapsto s(0)\}$
- $\sigma_2 := \{x \mapsto s(0)\}$

Feedback zur Vorlesung

Wir haben den Satz „Jede Boolesche Algebra ist isomorph zu EINER Mengenalgebra“ behandelt. Gibt es somit mehrere Mengenalgebren? Und was heißt isomorph?

Definition

Wir betrachten die Algebra $\langle \mathcal{P}(M); \cup, \cap, \sim, \emptyset, M \rangle$

- \cup die Mengenvereinigung; \cap die Schnittmenge; \sim die Komplementärmenge

Diese Algebra nennt man **Mengenalgebra**.

Bemerkung

Isomorphie bedeutet, dass die Operationen auf den Algebren ident sind; also ist jede Gleichheit in **einer** Mengenalgebra eine Gleichheit für **alle** Booleschen Algebren

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

algebraische Strukturen, Beispiele von Algebren, Zusammenhang Boolesche Algebra und Aussagenlogik, **Universelle Algebra**, **Satz von Birkhoff**

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

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare

Feedback zum Brückenkurs

Die Vorlesung zu "Wozu braucht man im Informatik-Studium Mathematik?" war für viele recht unverständlich. Außerdem war das Beispiel, warum man möglichst jeden Algorithmus mathematisch beweisen sollte, vollkommen ungerechtfertigt.

Zur Erklärung: [...] Der Autopilot von Tesla basiert auf einem Neuronen Netzwerk (NN) und ein NN lässt sich nicht mathematisch beweisen, weil NN ihre Funktionalität erlernen genauso wie ein Mensch etwas lernt. Selbst wenn der Autopilot auf normalen Algorithmen basieren würde, wie möchte man denn beweisen, dass eine Straßenverengung IMMER als Straßenverengung erkannt wird? [...] Es kann aber auch passieren, dass das NN die Straßenverengung nicht erkennt. In diesem Fall wird der Vorfall aufgezeichnet und das NN neu trainiert. Das ist auch der Grund, warum Tesla ihre Fahrzeuge mit einem "halbfertigen Autopilot herumfahren lässt: Damit sie möglichst viele Spezialfälle aufzeichnen, die wiederum durch das Training des NN den Autopilot sicherer machen. Falls sie mir nicht glauben, hier ist ein recht umfassendes Video, in dem erklärt wird, wie der Autopilot von Tesla funktioniert und auch wie der neue NN-Chip von Tesla aufgebaut ist: <https://www.youtube.com/watch?v=Ucp0TTmq0E>

Zu Neuronen Netzwerken siehe <https://frcr.acm.org/turing-lecture-at-frcr-2019>, bzw. 1:56 im Tesla Video

Beispiel (Gleichungen für Boolesche Ausdrücke: Revisited)

1 Wir betrachten die folgende Signatur

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

sodass

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

2 $V = \{x_1, x_2, \dots\}$

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 $E \vdash 1 + x \approx 1$

5 Aber es gilt auch $E \not\vdash x + 1 \approx 1$

Frage

1 Ist die Gleichungslogik **korrekt**?

Sind zum Beispiel alle Schlussfolgerungen aus den Gesetzen der Booleschen Algebra wirklich Äquivalenz 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

Definition

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

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

Bemerkung

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

Definition (Semantische Konsequenz)

- 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} schreiben wir $\mathcal{A} \models s \approx t$

Beispiel

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

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

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

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

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

Beispiel

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

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

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

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

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

Definition

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

- Eine Algebra \mathcal{A} heißt **Modell** von E , wenn jede Identität in E in \mathcal{A} gilt
- Gleichung $s \approx t$ ist **semantische Konsequenz** von E wenn gilt:

für alle Modelle \mathcal{A} von E : $\mathcal{A} \models s \approx t$

- Die Frage ob $E \models s \approx t$ heißt **Wortproblem**

$\mathcal{A} \models E$

$E \models s \approx t$

Beispiel

Sei E die Menge an Gleichungen:

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

- \mathcal{A} ist Modell von E ; \mathcal{B} ist **kein** Modell von E
- $E \not\models x + 1 \approx 1$, da Algebra \mathcal{C} existiert, sodass $\mathcal{C} \models E$, aber $\mathcal{C} \not\models x + 1 \approx 1$

Beispiel (Fortsetzung)

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

$+^B$	0	1	\sim^B		1^B	
0	0	0	0	1		1
1	1	1	1	1		

- Dann gilt $\mathcal{C} \models (x + y) + z \approx x + (y + z)$, $\mathcal{C} \models \sim(x) + x \approx 1$, $\mathcal{C} \models x + x \approx x$
- Also ist \mathcal{C} Modell von E
- Aber $\mathcal{C} \not\models x + 1 \approx 1$

Definition (Alphabet)

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

Beispiel

- $\Sigma = \{0, 1\}$ ist das **binäre** Alphabet
- $\Sigma = \{a, b, \dots, z\}$, 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, \dots bezeichnet
- Wörter werden mit x, y, z, \dots 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
- $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \dots$ 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, wir schreiben $x \cdot y$ für die **Konkatenation** von x und y : Sei $x = a_1 a_2 \cdots a_i$, $y = b_1 b_2 \cdots b_j$, dann gilt

$$x \cdot y = a_1 a_2 \cdots a_i b_1 b_2 \cdots b_j$$

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***