Grundlagen der Theoretischen Informatik

Sommersemester 2016

Viorica Sofronie-Stokkermans

e-mail: sofronie@uni-koblenz.de

0. Organisatorisches

Kontakt:

Viorica Sofronie-Stokkermans

sofronie@uni-koblenz.de

Raum B 225

Sprechstunde: Montag: 16:00 (Anmeldung über E-Mail)

Übung

Teresa Bergk

Webseite

Webseite:

http://userpages.uni-koblenz.de/∼sofronie/gti-ss-2016/

Alle relevante Information auf der Webseite

- Folien
- Weitere Materialien
- Termine usw.

Übung

http://userpages.uni-koblenz.de/∼sofronie/gti-ss-2016/uebung/gti16.html

Newsgroup: infko.theoinf

KLIPS: E-Mails (bitte melden Sie sich in KLIPS an!)

Vorlesung

4 Stunden/Woche

Termine:

- Mittwoch, 14:00 -16:00, Raum D028.
- Donnerstag, 14:00 -16:00, Raum M001.

14:00 s.t. oder 14:00 c.t. ?

Übungen

2 Stunden/Woche

- 2 Gruppen
  - Gruppe 1: Dienstag 12:00 c.t. in B016
  - Gruppe 2: Dienstag 16:00 s.t. in K208
- erste Übungsstunde:19.04.2016

Übungsblätter

- Übungszettel werden freitags auf der Webseite der Übung veröffentlicht.
- Besprechung der Übungszettel erfolgt in der darauf folgenden Woche in den Übungsstunden.
- Abgabe der Übungszettel ist nicht erforderlich.

Scheinvergabe

Klausur

- 1. Teilklausur (Dauer: 60 min)
  Voraussichtlich in der ersten oder zweiten Woche nach den Pfingstferien (1.06.2016 oder 8.06.2016)
- 2. Teilklausur 28. Juli 2016 (14:00-15:00, Raum D-028)
  Zulassung: bestandene Teilklausur

Wiederholung einzelner Teilklausuren nicht möglich

Nachklausur: Voraussichtlich am Ende des Semesters (September).

Nachklausur hat gleichen Wert wie alle Teilklausuren zusammen

Dauer: 120 min

Frage- und Antwortstunde: In der letzten Vorlesung (21.07.2016).

Literatur zur Vorlesung

Katrin Erk, und Lutz Priese (2008).
Theoretische Informatik: Eine umfassende Einführung.
3. Auflage.
Springer-Verlag.

Weitere Literatur

J. Hopcroft, R. Motwani, and J. Ullman (2002).
Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie.
Pearson.

U. Schöning (1994).
Theoretische Informatik: kurzgefaßt.
Spektrum-Verlag.

Dank

Diese Vorlesungsmaterialien basieren ganz wesentlich auf den Folien zu den Vorlesungen von

Katrin Erk (gehalten an der Universität Koblenz-Landau)

Jürgen Dix (gehalten an der TU Clausthal)

Bernhard Beckert (gehalten an der Universität Koblenz-Landau)

Ulrich Furbach (gehalten an der Universität Koblenz-Landau)

Ihnen gilt mein herzlicher Dank.

Motivation; Inhalt der Vorlesung

Theoretische Informatik befasst sich mit ...

Grundlegende Konzepte der Informatik

- Probleme und ihre Beschreibung
- Systeme/Automaten/Maschinen, die Probleme lösen
- Lösbarkeit von Problemen
  (Entscheidbarkeit/Berechenbarkeit und deren Grenzen)
- Schwierigkeit (Komplexität) der Lösung von Problemen

Teilgebiete der Theoretischen Informatik

- Formale Sprachen
- Automatentheorie
- Berechenbarkeitstheorie
- Komplexitätstheorie
- (Logik)

Warum Theoretische Informatik?

- ist die Grundlage
- ist wichtig
  (bspw. für Algorithmentechnik, Software Engineering, Compilerbau)
- hilft, weitere Themen/Vorlesungen der Informatik zu verstehen
- veraltet nicht
- macht Spaß

Inhalt der Vorlesung

1. Terminologie
2. Endliche Automaten und reguläre Sprachen
3. Kellerautomaten und kontextfreie Sprachen
4. Turingmaschinen und rekursiv aufzählbare Sprachen
5. Berechenbarkeit, (Un-)Entscheidbarkeit
6. Komplexitätsklassen P und NP

Kurzer Überblick: Logik

Logische Formeln

Aussagenlogische Operatoren

$\neg$ Negationssymbol („nicht“)

$\wedge$ Konjunktionssymbol („und“)

$\vee$ Disjunktionssymbol („oder“)

$\rightarrow$ Implikationssymbol („wenn . . . dann“)

$\leftrightarrow$ Symbol für Äquivalenz („genau dann, wenn“)

Zusätzliche prädikatenlogische Operatoren

$\forall$ Allquantor („für alle“)

$\exists$ Existenzquantor („es gibt“)

Logische Formeln

Formeln

- Atomare Aussagen sind Formeln
- Seien A, B Formeln, x eine Variable, dann sind

  $$\neg A, \quad (A \land B), \quad (A \lor B), \quad (A \rightarrow B), \quad (A \leftrightarrow B), \quad \forall x A, \quad \exists x A$$

  Formeln

Logische Formeln

Beispiele

$$\neg \underbrace{(y \leq x)}_{\text{Atom}} \rightarrow \exists z \underbrace{(\neg(z \leq x) \wedge \neg(y \leq z))}_{\text{Skopus von } \exists z}$$

Logische Formeln

Beispiele

„Alle, die in Koblenz studieren, sind schlau“

$$\underbrace{\forall \underbrace{x}_{\text{Variable}} \underbrace{(\mathit{studiertIn}(x, \mathit{koblenz}) \rightarrow \mathit{schlau}(x))}_{\text{Formel(Skopus)}}}_{\text{Formel}}$$

„Es gibt Jemand, der in Landau studiert und ist schlau“

$$\underbrace{\exists \underbrace{x}_{\text{Variable}} \underbrace{(\mathit{studiertIn}(x, \mathit{landau}) \land \mathit{schlau}(x))}_{\text{Formel(Skopus)}}}_{\text{Formel}}$$

Eigenschaften von Quantoren

Eigenschaften von Quantoren

Quantoren gleicher Art kommutieren

$\forall x \forall y$ ist das gleiche wie $\forall y \forall x$

$\exists x \exists y$ ist das gleiche wie $\exists y \exists x$

Eigenschaften von Quantoren

Verschiedene Quantoren kommutieren NICHT

$\exists x \forall y$ ist nicht das gleiche wie $\forall y \exists x$

Eigenschaften von Quantoren

Verschiedene Quantoren kommutieren NICHT

$\exists x \forall y$ ist nicht das gleiche wie $\forall y \exists x$

Beispiel

- $\exists x \forall y \; loves(x, y)$

- $\forall y \exists x \; loves(x, y)$

Eigenschaften von Quantoren

Verschiedene Quantoren kommutieren NICHT

$\exists x \forall y$ ist nicht das gleiche wie $\forall y \exists x$

Beispiel

- $\exists x \forall y \; loves(x, y)$

  Es gibt eine Person, die jeden Menschen in der Welt liebt (einschließlich sich selbst)

- $\forall y \exists x \; loves(x, y)$

  Jeder Mensch wird von mindestens einer Person geliebt

(Beides hoffentliche wahr aber verschieden:
das erste impliziert das zweite aber nicht umgekehrt)

Eigenschaften von Quantoren

Verschiedene Quantoren kommutieren NICHT

$\exists x \forall y$ ist nicht das gleiche wie $\forall y \exists x$

Beispiel

- $\forall x \exists y \; mutter(y, x)$

- $\exists y \forall x \; mutter(y, x)$

Eigenschaften von Quantoren

Verschiedene Quantoren kommutieren NICHT

$\exists x \forall y$ ist nicht das gleiche wie $\forall y \exists x$

Beispiel

- $\forall x \exists y \, mutter(y, x)$

  Jeder hat eine Mutter **(richtig)**

- $\exists y \forall x \, mutter(y, x)$

  Es gibt eine Person, die die Mutter von jedem ist **(falsch)**

Eigenschaften von Quantoren

Dualität der Quantoren

$\forall x \ \ldots$ ist das gleiche wie $\neg\exists x\, \neg \ldots$

$\exists x \ \ldots$ ist das gleiche wie $\neg\forall x\, \neg \ldots$

Eigenschaften von Quantoren

Dualität der Quantoren

$\forall x \ \ldots$ ist das gleiche wie $\neg \exists x \neg \ldots$

$\exists x \ \ldots$ ist das gleiche wie $\neg \forall x \neg \ldots$

Beispiel

- $\forall x \ mag(x, eiscreme)$ ist das gleiche wie $\neg \exists x \ \neg mag(x, eiscreme)$
- $\exists x \ mag(x, broccoli)$ ist das gleiche wie $\neg \forall x \ \neg mag(x, broccoli)$

Eigenschaften von Quantoren

$\forall$ **distributiert über** $\wedge$

$\exists$ **distributiert über** $\vee$

Eigenschaften von Quantoren

$\forall$ distributiert NICHT über $\vee$

$\forall x\,(\ldots \vee \ldots)$ ist NICHT das gleiche wie $(\forall x \ldots) \vee (\forall x \ldots)$

Eigenschaften von Quantoren

$\forall$ distributiert NICHT über $\vee$

$\forall x\ (\ldots \vee \ldots)$ ist NICHT das gleiche wie $(\forall x \ldots) \vee (\forall x \ldots)$

Beispiel

$\forall x\ (\mathit{eiscreme}(x) \vee \mathit{broccoli}(x))$
ist NICHT das gleiche wie
$(\forall x\ \mathit{eiscreme}(x)) \vee (\forall x\ \mathit{broccoli}(x))$

Eigenschaften von Quantoren

$\exists$ distributiert NICHT über $\wedge$

$\exists x\ (\ldots \wedge \ldots)$ ist NICHT das gleiche wie $(\exists x \ldots) \wedge (\exists x \ldots)$

Eigenschaften von Quantoren

$\exists$ distributiert NICHT über $\wedge$

$\exists x\ (\ldots \wedge \ldots)$ ist NICHT das gleiche wie $(\exists x \ldots) \ \wedge \ (\exists x \ldots)$

Beispiel

$\exists x\ (\mathit{gerade}(x) \wedge \mathit{ungerade}(x))$ ist NICHT das gleiche wie
$(\exists x\ \mathit{gerade}(x)) \ \wedge \ (\exists x\ \mathit{ungerade}(x))$

Beispiele: Familienverhältniss

- „Brüder sind Geschwister“
- „bruder“ ist symmetrisch
- „Mütter sind weibliche Elternteile“
- „Ein Cousin ersten Grades ist
  das Kind eines Geschwisters eines Elternteils“

Beispiele: Familienverhältniss

- „Brüder sind Geschwister“
  $\forall x \forall y\ (\mathit{bruder}(x, y) \rightarrow \mathit{geschwister}(x, y))$
- „bruder“ ist symmetrisch
- „Mütter sind weibliche Elternteile“
- „Ein Cousin ersten Grades ist
  das Kind eines Geschwisters eines Elternteils“

Beispiele: Familienverhältniss

- „Brüder sind Geschwister“
  $\forall x \forall y\ (\mathit{bruder}(x, y) \rightarrow \mathit{geschwister}(x, y))$
- „bruder“ ist symmetrisch
  $\forall x \forall y\ (\mathit{bruder}(x, y) \leftrightarrow \mathit{bruder}(y, x))$
- „Mütter sind weibliche Elternteile“
- „Ein Cousin ersten Grades ist
  das Kind eines Geschwisters eines Elternteils“

Beispiele: Familienverhältniss

- „Brüder sind Geschwister“
  $\forall x \forall y\ (\mathit{bruder}(x, y) \rightarrow \mathit{geschwister}(x, y))$
- „bruder“ ist symmetrisch
  $\forall x \forall y\ (\mathit{bruder}(x, y) \leftrightarrow \mathit{bruder}(y, x))$
- „Mütter sind weibliche Elternteile“
  $\forall x \forall y\ (\mathit{mutter}(x, y) \leftrightarrow \mathit{weiblich}(x) \wedge \mathit{elter}(x, y)))$
- „Ein Cousin ersten Grades ist
  das Kind eines Geschwisters eines Elternteils“

Beispiele: Familienverhältniss

- „Brüder sind Geschwister“
  $\forall x \forall y\ (\mathit{bruder}(x, y) \rightarrow \mathit{geschwister}(x, y))$
- „bruder“ ist symmetrisch
  $\forall x \forall y\ (\mathit{bruder}(x, y) \leftrightarrow \mathit{bruder}(y, x))$
- „Mütter sind weibliche Elternteile“
  $\forall x \forall y\ (\mathit{mutter}(x, y) \leftrightarrow \mathit{weiblich}(x) \wedge \mathit{elter}(x, y)))$
- „Ein Cousin ersten Grades ist
  das Kind eines Geschwisters eines Elternteils“
  $\forall x \forall y\ (\mathit{cousin}1(x, y) \leftrightarrow \exists p \exists ps\ (\mathit{elter}(p, x) \wedge \mathit{geschwister}(ps, p) \wedge \mathit{elter}(ps, y)))$

Beispiele: Familienverhältniss

Formalisierung von „Bruder, der nicht nur Halbbruder ist“

$$
\begin{aligned}
\forall x \forall y\ \mathit{bruder}(x, y) \ \leftrightarrow\ (&\neg(x = y) \wedge \\
&\exists m \exists v\ (\neg(m = v) \wedge \\
&\qquad \mathit{elter}(m, x) \wedge \mathit{elter}(v, x) \wedge \\
&\qquad \mathit{elter}(m, y) \wedge \mathit{elter}(v, y)))
\end{aligned}
$$

Kurzer Überblick:

Beweismethoden und Mathematische Konzepte

Wichtige Beweismethoden

Deduktiver Beweis (Direkter Beweis)

- Aneinanderkettung von Argumenten/Aussagen

$$A = A_1, A_2, \ldots, A_n = B$$

- Zwischenaussagen A_i müssen schlüssig aus dem Vorhergehenden folgen
- Verwendet werden dürfen nur
  - Annahmen aus A
  - mathematische Grundgesetze
  - bereits bewiesene Aussagen
  - logische Schlussfolgerungen

Wichtige Beweismethoden

Deduktiver Beweis (Direkter Beweis)

Beispiel: Zu beweisen:

Wenn x die Summe der Quadrate von vier strikt positiven ganzen Zahlen ist, dann gilt $2^x \geq x^2$

Wichtige Beweismethoden

Deduktiver Beweis (Direkter Beweis)

Beispiel: Zu beweisen:
Wenn x die Summe der Quadrate von vier positiven ganzen Zahlen ist, dann gilt $2^x \geq x^2$

Beweis in schematischer Darstellung:

	Aussage	Begründung
1.	$x = a^2 + b^2 + c^2 + d^2$	Gegeben
2.	$a \geq 1, b \geq 1, c \geq 1, d \geq 1$	Gegeben
3.	$a^2 \geq 1, b^2 \geq 1, c^2 \geq 1, d^2 \geq 1$	(2) und Gesetze der Arithmetik
4.	$x \geq 4$	(1), (3) und Gesetze der Arithmetik
5.	$2^x \geq x^2$	(4) und Satz aus der Analysis

Wichtige Beweismethoden

Beweis durch Kontraposition

Um zu zeigen, dass B aus der Annahme A folgt,

beweise, dass nicht A aus der Annahme nicht B folgt:

$$\neg B \to \neg A \qquad \text{logisch äquivalent zu} \qquad A \to B$$

Wichtige Beweismethoden

Beweis durch Kontraposition

Um zu zeigen, dass B aus der Annahme A folgt,

beweise, dass nicht A aus der Annahme nicht B folgt:

$$\neg B \to \neg A \qquad \text{logisch äquivalent zu} \qquad A \to B$$

Widerspruchsbeweis

Um zu zeigen, dass B aus der Annahme A folgt,

beweise, dass aus A und nicht B ein Widerspruch folgt:

$$(A \land \neg B) \leftrightarrow \mathit{false} \qquad \text{logisch äquivalent zu} \qquad A \to B$$

Wichtige Beweismethoden

Beweis durch Kontraposition

Um zu zeigen, dass B aus der Annahme A folgt,

beweise, dass nicht A aus der Annahme nicht B folgt:

$$\neg B \to \neg A \qquad \text{logisch äquivalent zu} \qquad A \to B$$

Widerspruchsbeweis

Um zu zeigen, dass B aus der Annahme A folgt,

beweise, dass aus A und nicht B ein Widerspruch folgt:

$$(A \land \neg B) \leftrightarrow \mathit{false} \qquad \text{logisch äquivalent zu} \qquad A \to B$$

- A kann „leer“ ($\top$) sein
- Widerspruch zu $\forall$-Aussage gelingt durch Gegenbeispiel

Wichtige Beweismethoden

Beweis durch Kontraposition

Beispiel

Behauptung: Ist die Wurzel aus einer geraden natürlichen Zahl n eine natürliche Zahl, so ist diese gerade.

$$n \text{ gerade und } \sqrt{n} = k \in \mathbb{N} \to k \text{ gerade}$$

Beweis durch Kontraposition: Zu zeigen:

$$\sqrt{n} = k \in \mathbb{N} \text{ und } k \text{ ungerade } \to n \text{ ungerade.}$$

Beweis: Angenommen, $\sqrt{n} = k$ wäre ungerade. Dann $k = 2l + 1$, so $k^2 = 4l^2 + 4l + 1$, d.h. auch $k^2 = n$ ist ungerade, und das ist ein Widerspruch zu der Voraussetzung, dass n gerade ist.
Also ist die getroffene Annahme falsch, d.h., $\sqrt{n}$ ist gerade.

Wichtige Beweismethoden

Widerspruchsbeweis

Beispiel

Behauptung: $\sqrt{2} \notin \mathbb{Q}$.

Beweis: Wir nehmen an dass $\sqrt{2} \in \mathbb{Q}$ und somit $\sqrt{2} = \frac{p}{q}$ wobei der Bruch p/q in gekürzter Form vorliegt (d.h. p und q teilerfremde ganze Zahlen sind). Dann $\left(\frac{p}{q}\right)^2 = 2$, d.h: $p^2 = 2q^2$.

Da $2q^2$ eine gerade Zahl ist, ist auch p^2 gerade. Daraus folgt, dass auch p gerade ist, d.h. $p = 2r$ (wobei $r \in \mathbb{Z}$). Damit erhält man mit obiger Gleichung: $2q^2 = p^2 = (2r)^2 = 4r^2$, und hieraus nach Division durch 2: $q^2 = 2r^2$. Mit der gleichen Argumentation wie zuvor folgt, dass q^2 und damit auch q eine gerade Zahl ist. Da p und q durch 2 teilbar sind, erhalten wir einen Widerspruch zur Teilerfremdheit von p und q. Dieser Widerspruch zeigt, dass die Annahme, $\sqrt{2}$ sei eine rationale Zahl, falsch ist und daher das Gegenteil gelten muss. Damit ist die Behauptung, dass $\sqrt{2}$ irrational ist, bewiesen.

Wichtige Beweismethoden

Induktionsbeweise

Standardinduktion:

Gilt $A(0)$ und
folgt $A(i+1)$ aus $A(i)$,
dann gilt $A(n)$ für alle $n \in \mathbb{N}$

Vollständige Induktion:

Gilt $A(0)$ und
folgt $A(i+1)$ aus $A(0) \wedge \ldots \wedge A(i)$,
dann gilt $A(n)$ für alle $n \in \mathbb{N}$

Strukturelle Induktion (auf Datentypen wie Listen, Bäumen, Wörtern):

Gilt A für das Basiselement und
folgt die Gültigkeit von A für ein beliebiges Element aus der Gültigkeit von A für seine Unterelemente,
dann gilt A für alle Elemente.

Standardinduktion: Beispiel

Behauptung: Für alle $n \in \mathbb{N}$, $\sum_{i=0}^{n} 2 * i = n(n+1)$.

$$p(n): \quad \sum_{i=0}^{n} 2i = n(n+1)$$

(1)	Induktionsbasis:	Beweise $p(0)$ OK
(2)	Induktionsvoraussetzung:	Für ein beliebig gewähltes $n \in \mathbb{N}$ gilt $p(n)$: $\sum_{i=0}^{n} 2i = n(n+1)$
(3)	Induktionsschluss:	Folgere $p(n+1)$ aus $p(n)$ $p(n+1): \sum_{i=0}^{n+1} 2i = (n+1)(n+2)$.

Beweis: $\sum_{i=0}^{n+1} 2i = (\sum_{i=0}^{n} 2i) + 2(n+1) \overset{p(n)}{=} n(n+1) + 2(n+1) = (n+1)(n+2)$.

Vollständige Induktion: Beispiel

Satz: Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von (≥ 1)*Primzahlendarstellen*.
$p(n)$: $n \geq 2 \Rightarrow n$ lässt sich als Produkt von Primzahlen darstellen.

Beweis: Sei $n \in \mathbb{N}$, $n \geq 2$, beliebig gewählt.

Induktionsvoraussetzung: $p(k)$ gilt für alle $k < n$
Induktionsschluss: Folgere $p(n)$ aus der Induktionsvoraussetzung.

Fallunterscheidung:

Fall 1: n **Primzahl.** Dann lässt sich n als Produkt von Primzahlen darstellen $(n = n)$

Fall 2: n **keine Primzahl.** Dann $n = k_1 \cdot k_2$, mit $k_1, k_2 \in \mathbb{N}$, $k_1, k_2 \geq 2$.
Da aber $k_i < n, i = 1, 2$ ist nach Induktionsvoraussetzung bereits eine Darstellung als Produkt von Primzahlen für k_i bekannt.
Multipliziert man diese beiden Produkte miteinander, so erhält man eine Darstellung für n.

Strukturelle Induktion

Induktive Definition von Mengen:

Induktive Definition einer Menge M aus einer Basismenge B mit "Konstruktoren" in Σ.

(Konstruktoren sind Funktionssymbole; für $f \in \Sigma$, $a(f) \in \mathbb{N}$ ist die Stelligkeit von f.)

Basismenge:	B
Erzeugungsregel:	Wenn $f \in \Sigma$ mit Stelligkeit n und $e_1, \dots, e_n \in M$, dann gilt $f(e_1, \dots, e_n) \in M$.

M ist die kleinste Menge,

- die die Basismenge B enthält,
- mit der Eigenschaft, dass für alle $f \in \Sigma$ mit Stelligkeit n und alle $e_1, \dots, e_n \in M$: $f(e_1, \dots, e_n) \in M$.

Induktive Definitionen: Beispiele

(1) Menge $\mathbb{N}$ aller natürlichen Zahlen

Basismenge:	0
Erzeugungsregel:	Wenn $n \in \mathbb{N}$, dann gilt $n + 1 \in \mathbb{N}$

$\mathbb{N}$ ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält 0;

(2) für alle Elemente n, falls $n \in A$ so $n + 1 \in A$.

Das bedeutet, dass:

(1) $0 \in \mathbb{N}$

(2) Falls $n \in \mathbb{N}$ so $n + 1 \in \mathbb{N}$.

(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\mathbb{N} \subseteq A$.

Induktive Definitionen: Beispiele

(3) Bin : die Menge aller (vollständigen) binären Bäume

Basismenge:	$\circ$ Baum mit nur einem Knoten.
Erzeugungsregel:	Wenn $B_1, B_2 \in \text{Bin}$, dann ist auch $\text{Tree}(B_1, B_2) \in \text{Bin}$.

Bin ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält der Baum mit nur einem Knoten $\circ$.

(2) für alle Elemente B_1, B_2, falls $B_1, B_2 \in A$ so $\text{Tree}(B_1, B_2) \in A$.

Das bedeutet, dass:

(1) $\circ \in \text{Bin}$

(2) Falls $B_1, B_2 \in \text{Bin}$ so $\text{Tree}(B_1, B_2) \in \text{Bin}$.

(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\text{Bin} \subseteq A$.

Induktive Definitionen: Beispiele

(4) Menge aller aussagenlogischen Formeln

Basismenge: $\perp$ (falsch), $\top$ (wahr), $P_0, P_1, P_2, \ldots$ sind aussagenlogische Formeln (atomare Formeln)

Erzeugungsregel: Wenn F_1, F_2 aussagenlogische Formeln sind, dann sind auch $\neg F_1$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $F_1 \rightarrow F_2$, $F_1 \leftrightarrow F_2$ aussagenlogische Formeln

Strukturelle Induktion

Sei M die kleinste Menge mit folgenden Eigenschaften:

- M enthält die Basismenge B,
- für alle $f \in \Sigma$ mit Stelligkeit n und alle $e_1, \ldots, e_n \in M$: $f(e_1, \ldots, e_n) \in M$.

Zu zeigen: $\forall x \in M : P(x)$

(1) **Induktionsbasis:** Beweise, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt.

(2) Sei $e \in M$, $e \notin B$.

Dann $e = f(e_1, \ldots, e_n)$, mit $f \in \Sigma$ und $e_1, \ldots, e_n \in M$.

Induktionsvoraussetzung: Wir nehmen an, dass $P(e_1), \ldots, P(e_n)$ gelten.

Induktionsschluss: Folgere, dass $P(e)$ gilt.

Strukturelle Induktion

Satz. Falls:

(1) bewiesen werden kann, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt. (Induktionsbasis)

(2) falls $e = f(e_1, \dots, e_n)$ mit $f \in \Sigma$
unter der Annahme dass $P(e_1), \dots, P(e_n)$ gelten (Induktionsvoraussetzung)
wir beweisen können, dass auch $P(e)$ gilt (Induktionsschritt)

Dann gilt $P(m)$ für alle $m \in M$.

Beweis: Sei $A = \{e \mid P(e) \text{ wahr } \}$.

(1) Da bewiesen werden kann, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt, wissen wir, dass A die Basismenge B enthält.

(2) Da wir, aus der Annahme dass $P(e_1), \dots, P(e_n)$ wahr sind, beweisen können, dass auch $P(e)$ wahr ist, wissen wir, dass
falls $e_1, \dots, e_n \in A$, und $f \in \Sigma$ (mit Stelligkeit n), so $f(e_1, \dots, e_n)$ in A.

Da M die kleinste aller Mengen mit Eigenschaften (1) und (2) ist, folgt, dass $M \subseteq A = \{e \mid P(e) \text{ wahr } \}$, d.h. $\forall m \in M, P(m)$ wahr.

Mathematische Konzepte

Grundkonzepte (z.B. aus DAS)

- Elementare Mengentheorie
  - $\{x|P(x)\}$
  - $\cup$, $\cap$, $\setminus$
- Bezug zwischen Mengen, Relationen und Funktionen **(wichtig!)**
- Elementare Gesetze der Algebra
- Strukturen wie Listen, (endliche) Folgen, Graphen, Bäume
- Wörter (Strings)

Mathematische Konzepte

Funktionen

Funktion $f : S \to S'$: Abbildung zwischen den Grundmengen S und S', nicht unbedingt auf allen Elementen von S definiert

Definitionsbereich D $\quad D = \{x \in S \mid \exists y \in S' \text{ mit } (x, y) \in f\}$

Wertebereich W $\quad W = \{y \in S' \mid \exists x \in S \text{ mit } (x, y) \in f\}$

f eine totale Funktion: f für alle Elemente in S definiert

$$\forall x{\in}S\ \exists y{\in}W\ (x, y) \in f$$

$$(x, y) \in f \qquad \mapsto \qquad f(x) = y$$

Injektiv, surjektiv, bijektiv

Injektiv: $\forall x, y (f(x) = f(y) \to x = y)$

Surjektiv: $\forall y \in S' \exists x \in S : \quad f(x) = y$

Bijektiv: injektiv + surjektiv

Übersicht

- Organizatorisches
- Literatur
- Motivation und Inhalt
- Kurzer Überblick: Logik
- Kurzer Überblick: Beweismethoden und mathematische Konzepte