Teil I: Formale Grundlagen der Informatik I
Endliche Automaten und formale Sprachen

Teil II: Formale Grundlagen der Informatik II
Logik in der Informatik

Martin Otto

Professor für Mathematische Logik
und Grundlagen der Informatik

TUD, Fachbereich Mathematik

Sommer 2010

Inhalt

Inhalt: FGdI I

Literatur

J. Hopcroft, R. Motwani, and J. Ullman:
Introduction to Automata Theory, Languages, and Computation,
Addison-Wesley, 2nd ed., 2001.
(inzwischen auch in deutscher Ausgabe)

U. Schöning:
Theoretische Informatik – kurzgefasst,
Spektrum, 4. Aufl., 2001.

I. Wegener:
Theoretische Informatik – eine algorithmenorientierte Einführung,
Teubner, 1999.

H.R. Lewis and C.H. Papadimitriou:
Elements of the Theory of Computation,
Prentice Hall, 2nd ed., 1998.

Kapitel 0: Einführung und Beispiele

Transitionssysteme: Beispiel

Beispiel 0.0.1

Weckzeit-Kontrolle eines Weckers

Zustände: (h, m, q) $\quad \begin{cases} h \in \mathrm{H} = \{0, \ldots, 23\} \\ m \in \mathrm{M} = \{0, \ldots, 59\} \\ q \in \{\mathrm{SETH}, \mathrm{SETM}, \mathrm{NIL}, \mathrm{ERROR}\} \end{cases}$

Aktionen/Operationen: *seth*, *setm*, $+$, $-$, *set*, *reset*

Typische Transitionen z.B.:

$(h, m, \mathrm{NIL}) \xrightarrow{seth} (h, m, \mathrm{SETH})$ (in den H-Setzen Modus)

$(h, m, \mathrm{SETH}) \xrightarrow{set} (h, m, \mathrm{NIL})$ (Ende H-Setzen Modus)

$(h, m, \mathrm{SETH}) \xrightarrow{seth} (h, m, \mathrm{ERROR})$ (bereits in H-Setzen Modus)

$(h, m, \mathrm{NIL}) \xrightarrow{+} (h, m, \mathrm{ERROR})$ (da nicht in Setzen Modus)

$(h, m, \mathrm{SETH}) \xrightarrow{+} ((h+1) \bmod 24, m, \mathrm{SETH})$ (H vorstellen)

$(h, m, \mathrm{ERROR}) \xrightarrow{reset} (0, 0, \mathrm{NIL})$ (reset)

Transitionssysteme: Beispiel

Beispiel 0.0.2

Mann/Wolf/Hase/Kohl

Zustände:

Verteilungen von $\{m, w, h, k\}$ rechts/links
symbolisiert durch Objekte $[m, w, h, k\| \,], \ldots, [m, w\|h, k], \ldots$

"erlaubte" Zustände:

rechte und linke Seiten $\neq [w, h]$, $[h, k]$, $[w, h, k]$

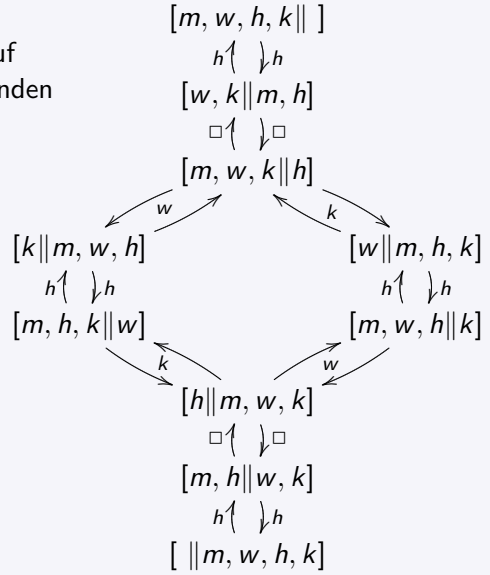
Transitionen: Änderung der Verteilung durch Bootsfahrten, z.B.

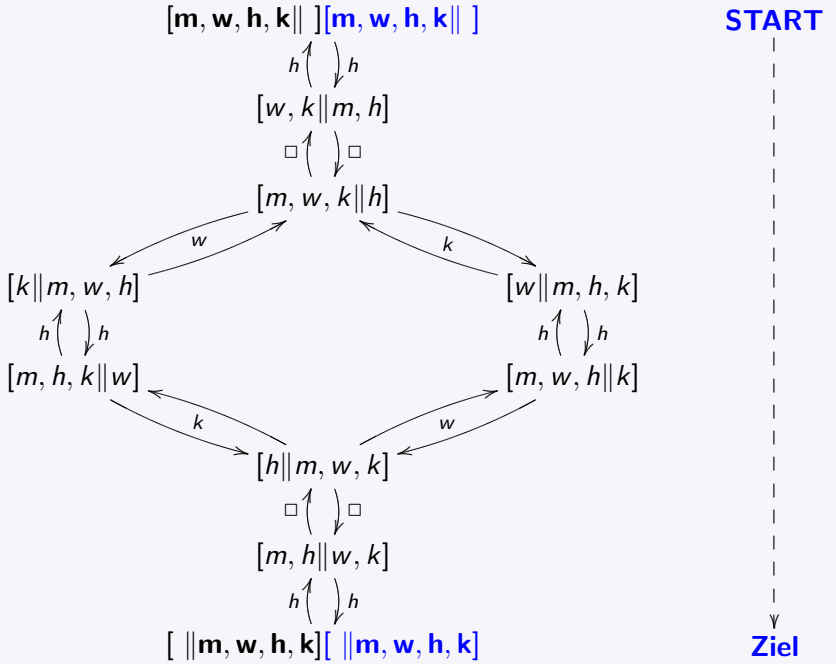
$[m, w, h, k\| \,] \xrightarrow{k} [w, h\|m, k]$ $\quad$ m transportiert k

$[m, w, h, k\| \,] \xrightarrow{\square} [w, h, k\|m]$ $\quad$ m fährt ohne Passagier

Mann/Wolf/Hase/Kohl

das vollständige Transitionssystem auf den erlaubten Zuständen





Alphabete/Wörter/Sprachen — Definition 0.0.3

Alphabet: nicht-leere, endliche Menge $\mathbf{\Sigma}$;
$a \in \Sigma$: Buchstabe/Zeichen/Symbol

$\mathbf{\Sigma}$-Wort: endliche Sequenz von Buchstaben aus Σ,
$\mathbf{w = a_1 \ldots a_n}$ mit $a_i \in \Sigma$

Menge aller $\mathbf{\Sigma}$-Wörter: $\mathbf{\Sigma^*}$

leeres $\mathbf{\Sigma}$-Wort: $\varepsilon \in \mathbf{\Sigma^*}$

$\mathbf{\Sigma}$-Sprache: Teilmenge $\mathbf{L} \subseteq \mathbf{\Sigma^*}$, eine Menge von Σ-Wörtern

Beispiel — Übung 0.0.4

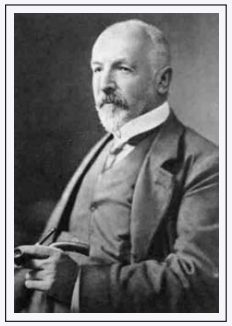
Σ Alphabet, $a \in \Sigma$.

Aufgabe: finde ein möglichst einfaches System, das auf einen (online fortlaufenden) Strom von Signalen aus Σ zu jedem Zeitpunkt die Information bereithält, ob die Anzahl der bisher eingetroffenen a durch 3 teilbar ist.

- a-Zähler mit Teilbarkeitstest?
- Reichen endlich viele Zustände?
  Wieviele mindestens?
- Wie verhält sich "Rest bzgl. Division durch 3" unter Konkatenation?

Kapitel 1: Mathematische Grundbegriffe
Mengen, Relationen, Funktionen, Strukturen, ...
elementare Beweistechniken

Georg Cantor (1845–1918)



Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen

Beispiele/Standardmengen

$\emptyset = \{\,\}$	die leere Menge
$\mathbb{B} = \{0,1\}$	Menge der Booleschen (Wahrheits)werte
$\mathbb{N} = \{0,1,2,\ldots\}$	Menge der natürlichen Zahlen (mit 0)
$\mathbb{Z}$ / $\mathbb{Q}$ / $\mathbb{R}$	Mengen der ganzen/rationalen/reellen Zahlen

Mengenbegriff (Cantor)

- *unstrukturierte* Sammlung von Objekten (Elementen);
  z.B. $A = \{a, b, c\} = \{b, a, a, c\}$
- die Gesamtheit ihrer Elemente legt die Menge fest (*Extensionalität*)
- über naiv aufzählende Spezifikation und die einfachsten Operationen hinausgehende Prinzipien (v.a. für die Existenz unendlicher Mengen)

  $\longrightarrow$ *axiomatische Mengenlehre* (Zermelo, Fraenkel, ZFC)

Mengen/Mengenoperationen → Abschnitt 1.1.1

Mengen $A, B, \ldots$

Elementbeziehung: $a \in A$ bzw. $a \notin A$ für "nicht $a \in A$"

Teilmengenbeziehung (Inklusion): $B \subseteq A$

z.B. $\emptyset \subseteq \{0,1\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$

Potenzmenge: $\mathcal{P}(A) = \{B\colon B \subseteq A\}$
die Menge aller Teilmengen von A

Mengengleichheit: $A = B$ gdw ($A \subseteq B$ und $B \subseteq A$)
[genau dieselben Elemente]
Extensionalität

Definition von Teilmengen: $B := \{a \in A\colon p(a)\}$
für eine Eigenschaft p

Boolesche Mengenoperationen

Durchschnitt: $A \cap B = \{c\colon c \in A \text{ und } c \in B\}$

A, B disjunkt gdw $A \cap B = \emptyset$

Vereinigung: $A \cup B = \{c\colon c \in A \text{ oder } c \in B\}$

Mengendifferenz: $A \setminus B = \{a \in A\colon a \notin B\}$

Komplement:
für Teilmengen einer festen Menge M, d.h. in $\mathcal{P}(M)$:

$\overline{B} := M \setminus B$ [Komplement bzgl. M]

Boolesche Mengenoperationen, Bemerkungen

große Vereinigungen/Durchschnitte über beliebige Familien von Mengen $(A_i)_{i\in I}$:

- $\bigcup_{i\in I} A_i = \{a\colon a \in A_i \text{ für mindestens ein } i \in I\}$
- $\bigcap_{i\in I} A_i = \{a\colon a \in A_i \text{ für alle } i \in I\}$

Beispiele: $\Sigma^* = \bigcup_{n\in\mathbb{N}} \Sigma^n$

$\Sigma^+ = \Sigma^* \setminus \{\varepsilon\} = \{w \in \Sigma^*\colon |w| \geqslant 1\} = \bigcup_{n\geqslant 1} \Sigma^n$

Tupel und Mengenprodukte

geordnete Paare: (a, b) mit erster Komponente a, zweiter Komponente b

n-Tupel: $(a_1, \ldots, a_n)$ mit n Komponenten $(n \in \mathbb{N}, n \geqslant 2)$

Kreuzprodukt (kartesisches Produkt):

$A \times B = \{(a, b)\colon a \in A, b \in B\}$

$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, \ldots, a_n)\colon a_i \in A_i \text{ für } 1 \leqslant i \leqslant n\}$

$A^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ mal}}$ Menge aller n-Tupel über A.

Bemerkung:
wir identifizieren n-Tupel über Σ mit Σ-Wörtern der Länge n und Wörter der Länge 1 mit Buchstaben, $\Sigma^1 = \Sigma$.

Relationen über einer Menge A

→ Abschnitt 1.1.2

n-stellige Relation: $R \subseteq A^n$
Menge von n-Tupeln über A

Beispiele: Kantenrelation eines Graphen, Präfixrelation auf Σ^*, Ordnungsrelationen, Äquivalenzrelationen, ...

Kantenrelationen in Graph/Transitionssystem:

$(u, v) \in E$ beschreibt E-Kante $u \xrightarrow{E} v$

Präfixrelation auf Σ^*:

$u \preccurlyeq v$ gdw. u Anfangsabschnitt (Präfix) von v

$\preccurlyeq = \{(u, uw)\colon u, w \in \Sigma^*\} \subseteq \Sigma^* \times \Sigma^*$

oft auch *infixe* Notation: aRb statt $(a, b) \in R$

Äquivalenzrelationen

wichtige potentielle Eigenschaften für 2-stelliges $R \subseteq A^2$:

Reflexivität: für alle $a \in A$ gilt: aRa.

Symmetrie: für alle $a, b \in A$ gilt: $aRb \Leftrightarrow bRa$.

Transitivität: für alle $a, b, c \in A$ gilt: (aRb und bRc) $\Rightarrow$ aRc.

z.B. Präfixrelation: reflexiv und transitiv, nicht symmetrisch

Äquivalenzrelation auf $R \subseteq A^2$:
reflexiv, **symmetrisch** und **transitiv**

Beispiele: Gleichheit (über A), Längengleichheit über Σ^*, gleicher Rest bei Division durch n über $\mathbb{N}$ oder $\mathbb{Z}$, ...

Idee: Äquivalenzrelationen als verallgemeinerte Gleichheiten

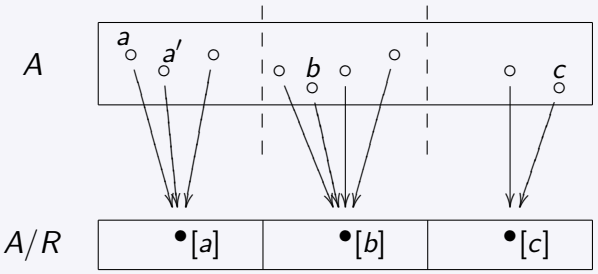
Äquivalenzklassen:

für Äquivalenzrelation $R \subseteq A^2$ auf A, $a \in A$:

$$[a]_R := \{b \in A \colon aRb\}$$
die **Äquivalenzklasse von a**

wichtig: A wird durch die Äquivalenzklassen in disjunkte Teilmengen zerlegt (Lemma 1.1.8), sodass

aRb gdw $[a]_R = [b]_R$



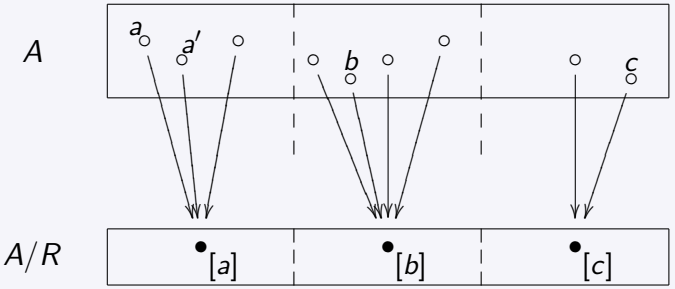
Äquivalenzrelationen: Quotient, natürliche Projektion

Quotient A/R : die Menge aller Äquivalenzklassen von R,

$$A/R := \{[a]_R \colon a \in A\}$$

die **natürliche Projektion**
$$\begin{array}{rcl} \pi_R \colon A & \longrightarrow & A/R \\ a & \longmapsto & [a]_R = \{b \in A \colon aRb\} \end{array}$$

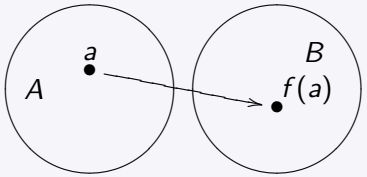
ordnet jedem Element seine Äquivalenzklasse zu



Funktionen und Operationen

→ Abschnitt 1.1.3

Funktion f von A nach B:
$$\begin{array}{rcl} f \colon A & \longrightarrow & B \\ a & \longmapsto & f(a) \end{array}$$



$f(a)$ ist das *Bild von* a unter f;
a ein *Urbild* von $b = f(a)$.

wesentlich: eindeutig definierter Funktionswert $f(a) \in B$ für jedes $a \in A$

A: **Definitionsbereich**

B: **Zielbereich**

$f(a)$ **Bild** von a unter f.

$f[A] := \{f(a) \colon a \in A\} \subseteq B$ **Bild(menge)** von f.

Funktionen, Operationen, Beispiele

n-stellige Funktion auf A: Funktion $f \colon A^n \to B$.

n-stellige Operation auf A: Funktion $f \colon A^n \to A$.

Beispiele: Addition, Multiplikation auf $\mathbb{N}$, $\mathbb{Z}$, ...

Beispiel **Konkatenation** auf Σ^*:
$$\begin{array}{rcl} \cdot \colon \Sigma^* \times \Sigma^* & \longrightarrow & \Sigma^* \\ (u, v) & \longmapsto & u \cdot v \ (= uv). \end{array}$$

Für $u = a_1 \dots a_n$; $v = b_1 \dots b_m$ ist $uv := \underbrace{a_1 \dots a_n}_{u} \underbrace{b_1 \dots b_m}_{v}$