Grundlagen der Theoretischen Informatik

Stefan Schirra

Fakultät für Informatik
Otto-von-Guericke Universität
Magdeburg

Wintersemester 2024/25

Die vorliegenden Folien sind ausschließlich für die Teilnehmer (m/w/d) an der Veranstaltung Grundlagen der Theoretischen Informatik im Wintersemester 2024/25 an der Otto-von-Guericke Universität Magdeburg bestimmt.

Grau, teurer Freund,
ist alle Theorie.

Organisatorisches

Vorlesung wöchentlich 3-stündig

donnerstags	9:15	-	10:00 Uhr
	10:15	-	11:00 Uhr
	11:15	-	12:00 Uhr

Übung wöchentlich 2-stündig

Anmeldung im moodle bis 21.10. 13:00 Uhr.

Prüfungsvoraussetzung

Erfolgreiche Teilnahme an den Übungen:

- Votieren für im Schnitt mindestens 50% der Aufgaben,
  genauer gesagt, für jeweils 4 aufeinanderfolgende Übungsblätter sind insgesamt 50% der Aufgaben dieser Blätter bis spätestens eine Stunde vor Übungsbeginn im moodle zu votierten, d.h. es müssen für die Übungsblätter 1, 2, 3 und 4 insgesamt 50% der Aufgaben dieser Blätter votiert werden, ebenso für die Blätter 2-5, 3-6, 4-7, ... und schließlich müssen auch für die letzen vier Übungsblätter 50% der Aufgaben dieser Blätter votiert werden.
- Mindestens zweimal erfolgreich eine eigene Lösung vortragen.

Die erfolgreiche Teilnahme an den Übungen ist Voraussetzung für die Teilnahme an der Prüfung.

Leistungsnachweis

Leistungsnachweiskriterien:

- erfolgreich an den Übungen teilnehmen, siehe oben, und
- entweder die Leistungsnachweisklausur nach dem aktuellen Semester oder deren Wiederholung nach dem darauf folgenden Semester bestehen.

Achtung: Wird keine dieser beiden Leistungsnachweisklausuren bestanden, so verfällt die erfolgreiche Teilnahme an den Übungen. Für einen Leistungsnachweis sind dann die Kriterien der nächsten Iteration der Vorlesung zu erbringen.

1

Einleitung

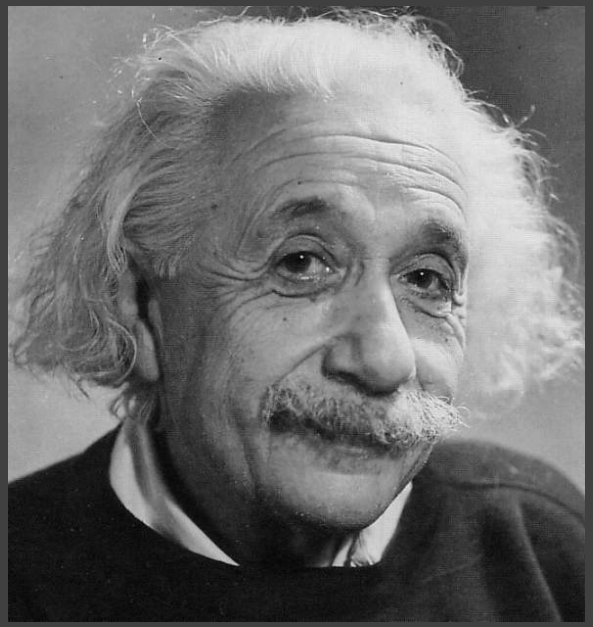
Theorie ?

abstrakte Gedanken und Vorstellungen, deren Bezug zur Realität nicht evident ist oder bezweifelt wird

> *Der Unterschied zwischen Theorie und Praxis ist in der Praxis weit höher als in der Theorie.*
>
> Ernst Ferstl

logisch-systematische Zusammenfassung und Verallgemeinerung von Erkenntnissen über einen Bereich der Wirklichkeit, deren Zusammenhänge erklärend, begründend widergespiegelt werden

- Spezielle Relativitätstheorie
- Newtonsche Theorie (klassische Mechanik)
- Quantentheorie
- Evolutionstheorie
- Wissenschaftstheorie



Es gibt nichts Praktischeres als eine gute Theorie!

Betrachtung der Wahrheit durch reines Denken,
unabhängig von ihrer Nutzbarmachung

Ein Theoretiker ist ein Mensch, der praktisch nur denkt.

Historisches

Beginn des 20. Jahrhunderts:
Ziel: Axiomatisierung der Mathematik

> *Diese Überzeugung von der Löslichkeit eines jeden mathematischen Problems ist uns ein kräftiger Ansporn während der Arbeit; wir hören in uns den steten Zuruf: Da ist das Problem, suche die Lösung. Du kannst sie durch reines Denken finden; denn in der Mathematik gibt es kein Ignorabimus!*
>
> David Hilbert, 1900

Emil du Bois-Reymond 1872: ignoramus et ignorabimus (Wir wissen es nicht und wir werden es niemals wissen): Skepsis gegenüber den Erklärungsansprüchen der Naturwissenschaften.

2. Hilbertsches Problem

2. Die Widerspruchslosigkeit der arithmetischen Axiome.

Wenn es sich darum handelt, die Grundlagen einer Wissenschaft zu untersuchen, so hat man ein System von Axiomen aufzustellen, welche eine genaue und vollständige Beschreibung derjenigen Beziehungen enthalten, die zwischen den elementaren Begriffen jener Wissenschaft stattfinden. Die aufgestellten Axiome sind zugleich die Definitionen jener elementaren Begriffe und jede Aussage innerhalb des Bereiches der Wissenschaft, deren Grundlagen wir prüfen, gilt uns nur dann als richtig, falls sie sich mittelst einer endlichen Anzahl logischer Schlüsse aus den aufgestellten Axiomen ableiten läßt. Bei näherer Betrachtung entsteht die Frage, ob etwa gewisse Aussagen einzelner Axiome sich untereinander bedingen und ob nicht somit die Axiome noch gemeinsame Bestandteile enthalten, die man beseitigen muß, wenn man zu einem System von Axiomen gelangen will, die völlig von einander unabhängig sind.

Vor Allem aber möchte ich unter den zahlreichen Fragen, welche hinsichtlich der Axiome gestellt werden können, dies als das wichtigste Problem bezeichnen, zu beweisen, daß dieselben untereinander widerspruchslos sind, d.h. daß man auf Grund derselben mittelst einer endlichen Anzahl von logischen Schlüssen niemals zu Resultaten gelangen kann, die miteinander in Widerspruch stehen.

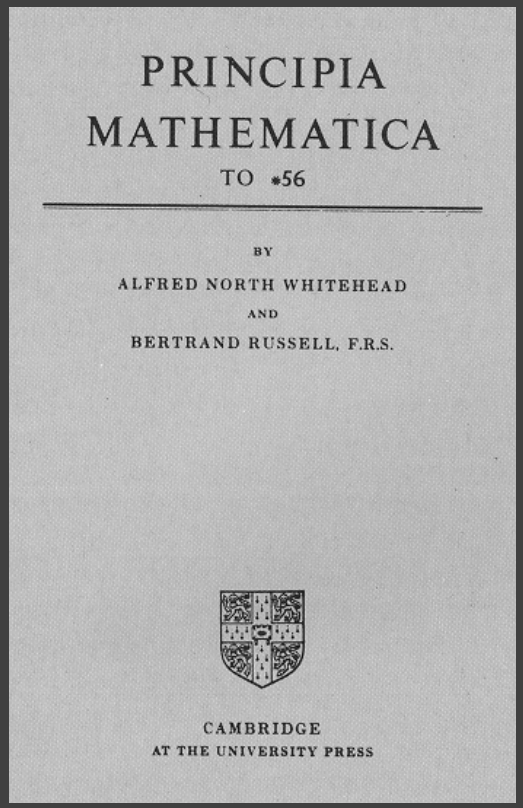
. . .

David Hilbert, 1900

Axiomatisierung

Whitehead, A. N., and B. Russell.
Principia Mathematica,
3 vols, Cambridge University Press,
1910, 1912, and 1913.

Second edition, 1925 (Vol. 1), 1927 (Vols 2, 3).
Abridged as Principia Mathematica to *56,
Cambridge University Press, 1962.


PRINCIPIA
MATHEMATICA
TO *56

BY
ALFRED NORTH WHITEHEAD
AND
BERTRAND RUSSELL, F.R.S.

CAMBRIDGE
AT THE UNIVERSITY PRESS

Russel-Zermelo Paradoxon (Russelsche Antinomie, 1903):

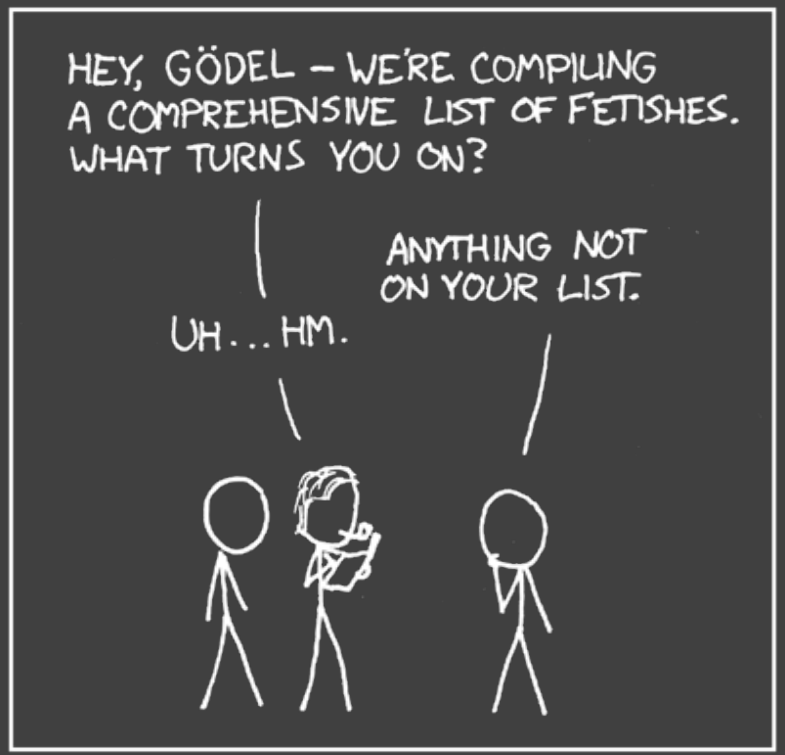
„Menge“ aller Mengen, die sich nicht selbst enthalten

$$\begin{aligned} R &= \{M \mid M \notin M\} \\ R \notin R &\Rightarrow R \in R \\ R \in R &\Rightarrow R \notin R \end{aligned}$$

$\rightarrow$ Zermelo-Fraenkel-Mengenlehre

AUTHOR KATHARINE GATES RECENTLY ATTEMPTED TO MAKE A CHART OF ALL SEXUAL FETISHES.

LITTLE DID SHE KNOW THAT RUSSELL AND WHITEHEAD HAD ALREADY FAILED AT THIS SAME TASK.



xkcd.com

Gödelscher Unvollständigkeitssatz

Satz: [Kurt Gödel, 1931]

Jedes Beweissystem für die Menge der wahren arithmetischen Formeln ist notwendigerweise unvollständig.

Es bleiben also immer wahre arithmetische Formeln übrig, die nicht beweisbar sind.

10. Hilbertsches Problem

10. Entscheidung der Lösbarkeit einer diophantischen Gleichung.

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

David Hilbert, 1900

Beweisen, dass man durch eine endliche Anzahl von Operationen
nach endlichen Raum, ob und wie viele ganzzahlige Lösungen
$\varphi(x, y, \ldots) = 0$ mit ganzzahligen Coefficienten besitzt.

David Hilbert, 1889

Entscheidungsprobleme

Entscheidungsproblem:

$$\mathcal{P} : \mathcal{I} \to \{\text{wahr}, \text{ falsch}\}$$

Das Entscheidungsproblem:
Gibt es einen Algorithmus, der für jede beliebige Formel der Prädikatenlogik erster Stufe entscheidet, ob die Formel allgemeingültig ist?

D. Hilbert, W. Ackermann, 1928


Null oder Eins, das ist hier die Frage.
19/2000
RITSCH-RENN.COM

Formalisierung des Berechenbarkeitsbegriffs

1920er, 1930er: "Effective Computability"

Berechnungsmodelle:

- λ-Kalkül
- Allgemeine rekursive Funktionen
- Turingmaschinen
- μ-rekursive Funktionen
- Postsche Systeme

Church, Gödel, Herbrand, Kleene, Post, Rosser, Turing, ...

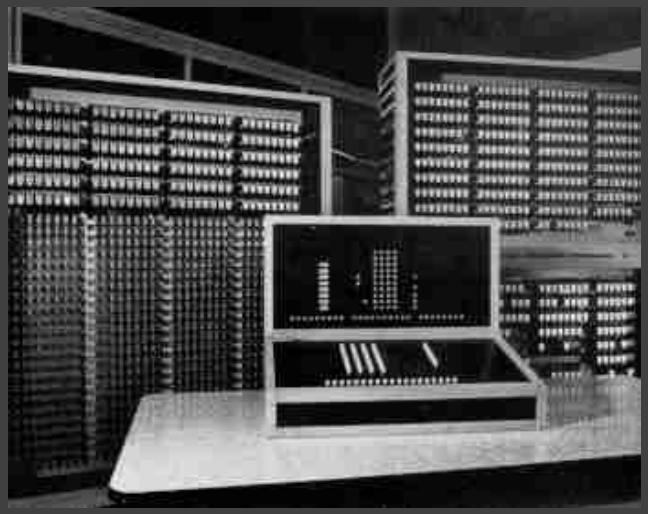
Turings Maschine

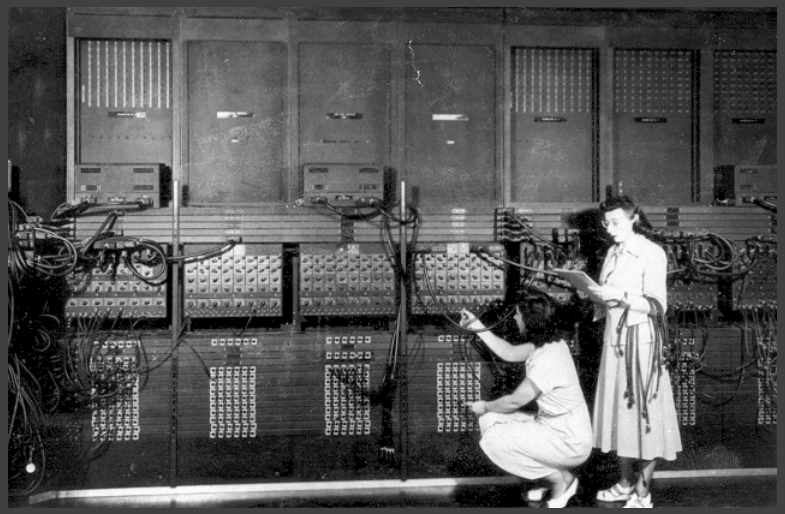
We may compare a man in the process of computing a real number to a machine which is only capable of a finite number of conditions $q_1, q_2, \ldots, q_R$ which will be called "m-configurations". The machine is supplied with a "tape" (the analogue of paper) running through it, and divided into sections (called "squares") each capable of bearing a "symbol". At any moment there is just one square, say the r-th, bearing the symbol $\mathfrak{S}(r)$ which is "in the machine". We may call this square the "scanned square". The symbol on the scanned square may be called the "scanned symbol". The "scanned symbol" is the only one of which the machine is, so to speak, "directly aware". However, by altering its m-configuration the machine can effectively remember some of the symbols which it has "seen" (scanned) previously. The possible behaviour of the machine at any moment is determined by the m-configuration q_n and the scanned symbol $\mathfrak{S}(r)$. This pair $q_n, \mathfrak{S}(r)$ will be called the "configuration": thus the configuration determines the possible behaviour of the machine. In some of the configurations in which the scanned square is blank (*i.e.* bears no symbol) the machine writes down a new symbol on the scanned square: in other configurations it erases the scanned symbol. The machine may also change the square which is being scanned, but only by shifting it one place to right or left. In addition to any of these operations the m-configuration may be changed. Some of the symbols written down

Churchsche These

Churchsche These [1936]:
Die Klasse der im intuitiven Sinne berechenbaren Funktionen stimmt genau mit der Klasse der Turing-berechenbaren Funktionen überein.

1940er, 1950er, 1960er, ...





- Computer (Z3, ENIAC, ...) und Programmiersprachen
- Markov-Algorithmen
- Registermaschinen
- WHILE-Programme

- Supercomputer

- Quantencomputer

. . . die Churchsche These hält stand . . .

Unentscheidbarkeit

Satz: [Church, 1936], [Turing, 1937]
Die Prädikatenlogik erster Stufe ist unentscheidbar.

Satz: [Yuri Matiyasevich, 1970]
Das 10. Hilbertsche Problem ist unlösbar.

Vorarbeiten von Julia Robinson, Martin Davis, Hilary Putnam, ...

Halteproblem

Halteproblem

Gegeben eine Turingmaschine (Beschreibung eines Programms) und eine endliche Eingabe für die Turingmaschine, entscheide, ob die Turingmaschine (das Programm) bei dieser Eingabe anhalten oder unendlich lange rechnen wird.

```
public static void main (String[] args) {
  int n = Integer.valueOf(args[0]).intValue();
  int total = 3;
  while (true) {
    for ( int x = 1; x <= total-2; ++x) {
      for ( int y = 1; y <= total-x-1; ++y) {
        int z = total - x - y;
        if ( exp(x,n) + exp(y,n) == exp(z,n) ) {
          return;
        }
      }
    }
    ++total;
  }
}
```

$$x^n + y^n = z^n$$

Satz: *Das Halteproblem ist nicht entscheidbar.*

Satz von Cook

entscheidbar $\not\Rightarrow$ handhabbar

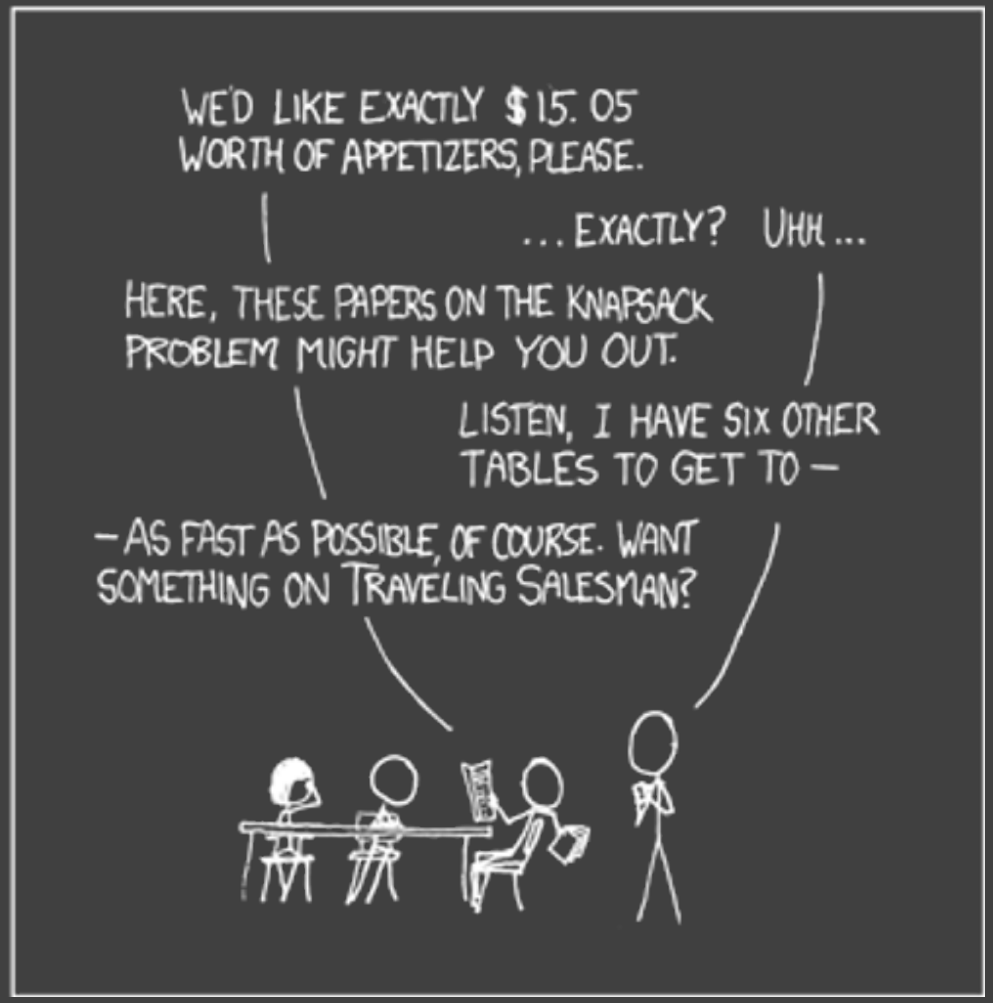
1970er: NP-Vollständigkeit

Wenn jemand einen Polynomialzeitalgorithmus für ein NP-vollständiges Problem findet, so hat er damit auch Polynomialzeitalgorithmen für alle anderen Probleme in der Klasse NP gefunden.

Satz: [Cook, 1971], [Levin, 1973]
Das Erfüllbarkeitsproblem der Aussagenlogik ist NP-vollständig.

MY HOBBY:

EMBEDDING NP-COMPLETE PROBLEMS IN RESTAURANT ORDERS



xkcd.com

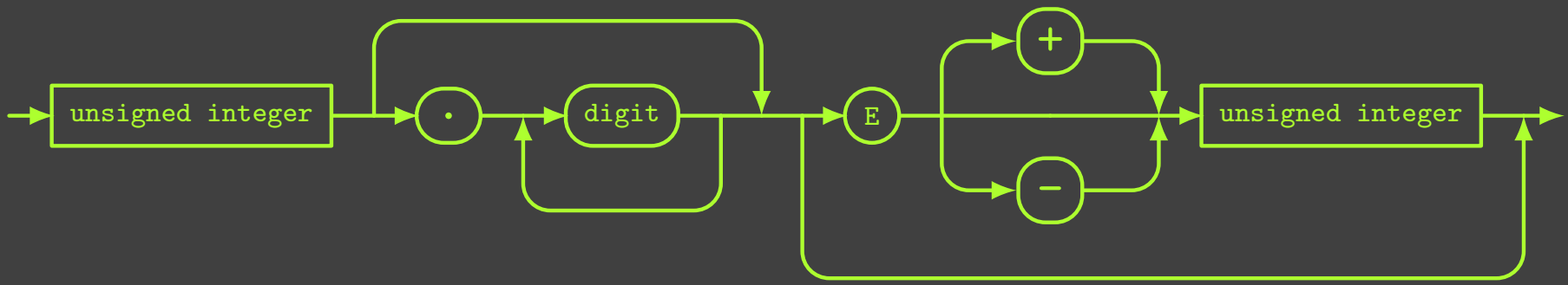
Formale Sprachen und Grammatiken

$$
\begin{aligned}
\langle \textit{Satz} \rangle &\rightarrow \langle \textit{Subjekt} \rangle \langle \textit{Prädikat} \rangle \langle \textit{Objekt} \rangle \\
\langle \textit{Subjekt} \rangle &\rightarrow \langle \textit{Artikel} \rangle \langle \textit{Attribut} \rangle \langle \textit{Substantiv} \rangle \\
\langle \textit{Artikel} \rangle &\rightarrow \text{der} \\
\langle \textit{Artikel} \rangle &\rightarrow \text{die} \\
\langle \textit{Artikel} \rangle &\rightarrow \ldots \\
\ldots &\rightarrow \ldots
\end{aligned}
$$

Blockdiagramme aus Beschreibung der PASCAL-Syntax

unsigned integer

unsigned real



Ausschnitt aus der Beschreibung der C++98-Syntax

```
class-name:
        identifier
        template-id
template-id:
        template-name < template-argument-list >
template-name:
        identifier
template-argument-list:
        template-argument
        template-argument-list , template-argument
identifier:
        nondigit
        identifier nondigit
        identifier digit
```

Wörter und Sprachen

Im Zusammenhang mit formalen Sprachen wird jede nichtleere endliche Menge als *Alphabet* bezeichnet. Die Elemente eines Alphabets werden *Symbole* genannt.

Ein *Wort* über einem Alphabet Σ ist eine endliche Folge von Symbolen aus Σ.

Das *leere Wort* ist die aus 0 Symbolen bestehende Folge und wird mit ε bezeichnet.

Die Menge aller Wörter über einem Alphabet Σ wird mit Σ^* bezeichnet. Ferner ist $\Sigma^+ = \Sigma^* - \{\varepsilon\}$.

Eine *Sprache* über einem Alphabet Σ ist eine Teilmenge von Σ^*.

Beispiele:

$\Sigma = \{a, b, c\}$

$$
\begin{aligned}
c &\in \Sigma^* \\
abba &\in \Sigma^* \\
cbc &\in \Sigma^* \\
abcca &\in \Sigma^* \\
\varepsilon &\in \Sigma^*
\end{aligned}
$$

$\{w \in \Sigma^* \mid w \text{ beginnt mit } a\}$

$\{w \in \Sigma^* \mid w \text{ enthält kein } c\}$

$\{w \in \Sigma^* \mid w \text{ enthält kein } a \text{ oder kein } b\}$

$\{w \in \Sigma^* \mid \text{die Anzahl der } a \text{ in } w \text{ ist eine Primzahl}\}$

$\emptyset \subseteq \Sigma^*$

Operationen auf Wörtern

Die *Länge* eines Wortes w ist die Länge der Folge der Symbole. Die Länge des Wortes w bezeichnen wir mit $|w|$.

Seien x und y Wörter über dem gleichen Alphabet. Dann bezeichnet $x \circ y$ das Wort, das durch Hintereinanderschreiben von x und y entsteht. Diese Operation wird als *Konkatenation* oder auch als Verkettung bezeichnet. Statt $x \circ y$ schreiben wir meist einfach xy.

Beispiel: $\mathit{kupfer} \circ \mathit{kessel} = \mathit{kupferkessel}$

Für alle Wörter u, v, w gilt

$$w \circ \varepsilon = \varepsilon \circ w = w$$

$$(u \circ v) \circ w = u \circ (v \circ w)$$

v ist *Teilwort* eines Wortes w, wenn es Wörter x und y gibt, so dass $w = xvy$.

v ist *Präfix* eines Wortes w, wenn es ein Wort y gibt, so dass $w = vy$.

v ist *Suffix* eines Wortes w, wenn es ein Wort x gibt, so dass $w = xv$.

Für ein Wort w und eine natürliche Zahl n bezeichnet w^n die n-fache Konkatenation von w:

$$w^1 = w$$
$$w^n = w^{n-1}w$$

und insbesondere

$$w^0 = \varepsilon$$

Beispiel: $(da)^3 = dadada$

w^n wird auch als *n-te Potenz* von w bezeichnet.

Für ein Wort w bezeichnet w^R das Wort w in umgekehrter Symbolfolge:

$$w = \sigma_1 \sigma_2 \cdots \sigma_k, \quad \sigma_i \in \Sigma, \qquad w^R = \sigma_k \sigma_{k-1} \cdots \sigma_1$$

Beispiel: $(magdeburg)^R = grubedgam$

w^R wird auch als *Spiegelung* von w bezeichnet.

R steht hier für die englische Bezeichnung *Reversal*.

Operationen auf Sprachen

Wie auf allen Mengen sind auch auf Sprachen die Operationen $\cup, \cap, -$ (Vereinigung, Schnitt, Differenz) definiert.

Das *Komplement* einer Sprache L über Σ enthält genau die Wörter aus Σ^*, die nicht zu L gehören. Wir bezeichnen das Komplement von L mit $\overline{L}$.

Seien L_1 und L_2 Sprachen über Σ. Dann ist $L_1 \circ L_2 = L_1 L_2 = \{w \in \Sigma^* \mid \text{es gibt } x \in L_1 \text{ und } y \in L_2 \text{ so dass } w = xy\}$ die *Konkatenation* von L_1 und L_2. Mit $L^n = \{w \in \Sigma^* \mid \text{es gibt } w_1, w_2, \ldots, w_n \in L \text{ so dass } w = w_1 w_2 \cdots w_n\}$ bezeichnen wir die n-te Potenz der Sprache L. Insbesondere ist $L^0 = \{\varepsilon\}$.

Der *Kleene Star* Abschluss einer Sprache L ist

$$L^* = \bigcup_{i \geq 0} L^i$$

Ferner definieren wir

$$L^+ = \bigcup_{i \geq 1} L^i$$

Schließlich definieren wir die Spiegelung einer Sprache L:

$$L^R = \{w^R \mid w \in L\}$$

Grammatik

Eine Grammatik generiert Wörter durch einen Termersetzungsprozess.

Definition:
Eine Grammatik ist ein 4-Tupel (V, Σ, R, S), wobei gilt:

- $V \neq \emptyset$ *ist eine endliche Menge, die Menge der* Nichtterminal(symbol)e *oder* Variablen,
- Σ *ist ein Alphabet, das* Terminalalphabet, $\Sigma \cap V = \emptyset$,
- $R \subset (V \cup \Sigma)^+ \times (V \cup \Sigma)^*$ *ist eine endliche Menge von* Regeln *oder auch* Produktionen,
- $S \in V$ *ist das* Startsymbol.

Falls $G = (V, \Sigma, R, S)$ eine Grammatik ist und $(u, v) \in R$,
so schreiben wir $u \to_G v$.

Beispiel: $G = (\{S\}, \{a, b\}, \{(S, \varepsilon), \quad (S, SS), \quad (S, aSb)\}, S)$

	S	Regel
$\Rightarrow_G$	SS	$S \to_G SS$
$\Rightarrow_G$	$aSbS$	$S \to_G aSb$
$\Rightarrow_G$	$aSSbS$	$S \to_G SS$
$\Rightarrow_G$	$aSSbaSb$	$S \to_G aSb$
$\Rightarrow_G$	$aaSbSbaSb$	$S \to_G aSb$
$\Rightarrow_G$	$aaSbSbab$	$S \to_G \varepsilon$
$\Rightarrow_G$	$aabSbab$	$S \to_G \varepsilon$
$\Rightarrow_G$	$aabaSbbab$	$S \to_G aSb$
$\Rightarrow_G$	$aababbab$	$S \to_G \varepsilon$

Zu einer gegebenen Grammatik $G = (V, \Sigma, R, S)$ definieren wir eine Relation $\Rightarrow_G$ auf $(V \cup \Sigma)^* \times (V \cup \Sigma)^*$ wie folgt: Seien $x, y \in (V \cup \Sigma)^*$.

$x \Rightarrow_G y$ genau dann wenn es $u, v, w, z \in (V \cup \Sigma)^*$ gibt, so dass

$$x = uvw, \quad y = uzw, \quad \text{und} \quad v \to_G z$$

Wir sagen, *x geht unter G unmittelbar in y über*, falls $x \Rightarrow_G y$.

Die *von* einer Grammatik G *erzeugte Sprache* ist

$$L(G) = \{w \in \Sigma^* \mid \exists w_1, \ldots, w_k : S \Rightarrow_G w_1 \Rightarrow_G w_2 \Rightarrow_G \cdots \Rightarrow_G w_k = w\}$$

Beispiel:

$$G = (\{S\}, \{a,b\}, \{S \to \varepsilon, \quad S \to SS, \quad S \to aSb\}, S)$$

$$\begin{aligned} ab &\in L(G) \\ ba &\notin L(G) \\ abab &\in L(G) \\ aabbab &\in L(G) \\ aabbba &\notin L(G) \end{aligned}$$

$L(G)$: korrekt verschachtelte „Klammern“

Beispiel:

$G = (\{S,A,B,C\},\{a,b,c\},R,S)$ mit

$$\begin{aligned} R \quad = \quad & \{S \to ABCS, \quad S \to \varepsilon, \\ & CA \to AC, \quad AC \to CA, \\ & BA \to AB, \quad AB \to BA, \\ & CB \to BC, \quad BC \to CB, \\ & A \to a, \ B \to b, C \to c\} \end{aligned}$$

$$L(G) = \{w \in \{a,b,c\}^* \mid w \text{ enthält gleichviele } a,b \text{ und } c\}$$

		Regel
	S	
$\Rightarrow_G$	$ABCS$	$S \to ABCS$
$\Rightarrow_G$	$ABCABCS$	$S \to ABCS$
$\Rightarrow_G$	$ABCABC$	$S \to \varepsilon$
$\Rightarrow_G$	$ABCBAC$	$AB \to BA$
$\Rightarrow_G$	$ABCBCA$	$AC \to CA$
$\Rightarrow_G$	$ABCCBA$	$BC \to CB$
$\Rightarrow_G$	$aBCCBA$	$A \to a$
$\Rightarrow_G$	$abCCBA$	$B \to b$
	$\vdots$	
$\Rightarrow_G$	$abccba$	

Chomsky-Hierarchie

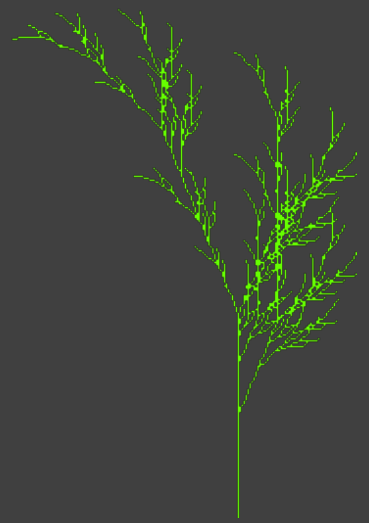
Klassifikation von Grammatiken (und daraus resultierend Klassifikation von formalen Sprachen)

- Typ 0 *allgemeine Grammatiken*
- Typ 1 *kontextsensitive Grammatiken*
- Typ 2 *kontextfreie Grammatiken*
- Typ 3 *reguläre Grammatiken*

Anwendungen

Formale Sprachen und Automatentheorie

- Textmustererkennung
- Programmiersprachendesign und Übersetzerbau
- Computergrafik: Pflanzengenerierung



Komplexitätstheorie

- Kryptographie

Autor: Bernd Lintermann

Auswirkungen

Berechenbarkeitstheorie

- Programmverifikation

Komplexitätstheorie

- Heuristiken und Approximationsalgorithmen

Überblick

1. Einleitung
2. Automatentheorie und Formale Sprachen
3. Berechenbarkeitstheorie
4. Komplexitätstheorie

Literaturhinweise

J. Hopcroft, R. Motwani, J. Ullmann.
Introduction to Automata Theory, Languages, and Computation (3rd Edition.).
Pearson – Addison-Wesley.

H. Lewis, C. Papadimitriou.
Elements of the Theory of Computation (2nd Edition).
Pearson – Prentice Hall.

E. Rich.
Automata, Computability, and Complexity.
Pearson – Prentice Hall.

M. Sipser.
Introduction to the Theory of Computation (2nd Edition).
Cengage Learning – Thomson.

U. Schöning.
Theoretische Informatik - kurzgefasst.
Spektrum.

B. Hollas.
Grundkurs Theoretische Informatik.
Spektrum.

R. Socher.
Theoretische Grundlagen der Informatik.
Hanser.

K. Erk, L. Priese.
Theoretische Informatik (3., erweiterte Auflage).
Springer Verlag.

D. W. Hoffmann.
Theoretische Informatik.
Hanser.

J. Hopcroft, R. Motwani, J. Ullmann.
Einführung in der Automatentheorie, Formale Sprachen und Komplexitätstheorie (2., überarbeitete Auflage).
Pearson Studium.

J. Hromkovic.
Theoretische Informatik: Formale Sprachen, Berechenbarkeit, Komplexitätstheorie, Algorithmik, Kommunikation und Kryptographie.
B.G.Teubner.

I. Wegener.
Theoretische Informatik – eine algorithmenorientierte Einführung.
B.G.Teubner.

I. Wegener.
Kompendium Theoretische Informatik – eine Ideensammlung.
B.G.Teubner.

D. Kozen.
Automata and Computability.
Springer Verlag.

P. Linz.
Introduction to Formal Languages and Automata (4th Edition).
Jones & Bartlett Publishers.

H. Chen.
Computability and Complexity.
The MIT Press.

Populärwissenschaftliches zum Thema:

D. Hofstadter.
Gödel, Escher, Bach: Ein Endloses Geflochtenes Band.
DTV.

D. Harel.
Das Affenpuzzle und weitere bad news aus der Computerwelt.
Springer Verlag.

Grundlagen

Notation:

Wir schreiben

$\neg$	für	*nicht*
$\vee$	für	*oder*
$\wedge$	für	*und*
$\Rightarrow$	für	*wenn . . . dann*
$\Leftrightarrow$	für	*genau dann wenn*
$\exists$	für	*es existiert*
$\forall$	für	*für alle*

Altgriechische Buchstaben

α	alpha	A	ν	ny	N
β	beta	B	ξ	xi	Ξ
γ	gamma	Γ	o	omikron	O
δ	delta	Δ	π	pi	Π
ε	epsilon	E	ρ	rho	P
ζ	zeta	Z	σ	sigma	Σ
η	eta	H	τ	tau	T
θ	theta	Θ	υ	ypsilon	Υ
ι	iota	I	ϕ	phi	Φ
κ	kappa	K	χ	chi	X
λ	lambda	Λ	ψ	psi	Ψ
μ	my	M	ω	omega	Ω

Mengenlehre

Eine *Menge* ist eine Zusammenfassung von *verschiedenen* Objekten zu einer Gesamtheit. Die Objekte in einer Menge werden *Elemente* der Menge genannt. Die Elemente sind ungeordnet, aber wohlunterschieden. Falls x ein Element einer Menge M ist, schreiben wir $x \in M$, sonst $x \notin M$.

$\emptyset$	leere Menge
$\mathbb{N}$	Menge der natürlichen Zahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}$	Menge der rationalen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{N}_0$	Menge der natürlichen Zahlen und Null

Darstellung von Mengen:

Aufzählung der Elemente:

$\{3,5,8,9,17\}$,

$\{a,b,c,d,e,f,g,h\}$,

$\{\text{grün}, \bullet, 61, \heartsuit, \{g,h\}\}$,

$\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$,

$\{0,1,4,9,16,25,\ldots\}$

Auswahl durch Eigenschaft:

$\{x \in M \mid \text{ und } x \text{ hat Eigenschaft } E\}$

$\{x \in \mathbb{N} \mid \text{ und } x \text{ ist ein Vielfaches von } 3\}$,

$\{x \in \mathbb{Z} \mid \text{ und } x \text{ ist gerade}\}$,

$\{x \in \mathbb{R} \mid \text{ und } x \text{ ist algebraisch}\}$

Eine Menge A heißt *Teilmenge* einer Menge B, wir schreiben $A \subseteq B$, falls jedes Element von A auch ein Element von B ist.

Eine Menge A heißt *Obermenge* einer Menge B, wir schreiben $A \supseteq B$, genau dann wenn $B \subseteq A$.

Zwei Mengen A und B heißen *gleich*, wir schreiben $A = B$, genau dann wenn $A \subseteq B$ und $B \subseteq A$ gilt.

Eine Menge A heißt *echte Teilmenge* einer Menge B, wir schreiben $A \subset B$, genau dann wenn $A \subseteq B$ und $A \neq B$.

$A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$ heißt *Vereinigung* von A und B

$A \cap B = \{x \mid x \in A \text{ und } x \in B\}$ heißt *Durchschnitt* von A und B

$A - B = \{x \mid x \in A \text{ und } x \notin B\}$ heißt *Differenz* von A und B

$2^A = \{M \mid M \subseteq A\}$, die Menge aller Teilmengen von A,
heißt *Potenzmenge* von A.

Satz: *Seien A, B und C Mengen. Dann gilt*

$$
\begin{aligned}
A \cup A &= A \\
A \cap A &= A \\
A \cup B &= B \cup A \\
A \cap B &= B \cap A \\
(A \cup B) \cup C &= A \cup (B \cup C) \\
(A \cap B) \cap C &= A \cap (B \cap C) \\
(A \cup B) \cap C &= (A \cap C) \cup (B \cap C) \\
(A \cap B) \cup C &= (A \cup C) \cap (B \cup C) \\
(A \cup B) \cap A &= A \\
(A \cap B) \cup A &= A \\
A - (B \cup C) &= (A - B) \cap (A - C) \\
A - (B \cap C) &= (A - B) \cup (A - C)
\end{aligned}
$$

Zwei Mengen A und B heißen *disjunkt*, falls sie keine gemeinsamen Elemente enthalten, d.h., falls $A \cap B = \emptyset$.

Eine Teilmenge Π der Potenzmenge 2^A einer nichtleeren Menge A heißt *Partition* von A, falls gilt

- jedes Element von Π ist nicht leer
- $B, C \in \Pi, B \neq C \Rightarrow B \cap C = \emptyset$
- jedes Element von A ist in einer der Mengen in Π enthalten

Eine *Folge* von Objekten ist eine Auflistung dieser Objekte in einer bestimmten Ordnung.

Ein *geordnetes n-Tupel* ist eine Folge von n Objekten. Wir schreiben

$$(a_1, a_2, \ldots, a_n)$$

Das i-te Objekt a_i der Folge wird als *i-te Komponente* bezeichnet. Ein *geordnetes Paar* ist ein geordnetes 2-Tupel.

Das *kartesische Produkt* $A_1 \times A_2 \times \cdots \times A_n$ von n Mengen $A_1, \ldots, A_n$ ist die Menge aller geordneten n-Tupel $(a_1, a_2, \ldots, a_n)$ mit $a_i \in A_i$ für alle $i = 1, \ldots, n$.

Relationen und Funktionen

Eine *n-stellige Relation* auf den Mengen $A_1, \ldots, A_n$ ist eine Teilmenge von $A_1 \times A_2 \times \cdots \times A_n$.

Eine 1-stellige Relation heißt *unäre Relation*, eine 2-stellige Relation heißt *binäre Relation*.

Eine *Funktion* von A nach B ist eine binäre Relation mit der Eigenschaft: Für jedes Element a aus A gibt es genau ein geordnetes Paar mit a als erster Komponente.

$$f : A \to B$$

$$a \mapsto f(a)$$

Eine *partielle Funktion* von A nach B ist eine binäre Relation mit der Eigenschaft: Für jedes Element a aus A gibt es höchstens ein geordnetes Paar mit a als erster Komponente.

Eine Funktion $f : A_1 \times A_2 \times \cdots \times A_n \to B$
mit $f(a_1, a_2, \ldots, a_n) = b$ heißt *n-stellige Funktion*. b heißt *Funktionswert*, die a_i werden *Argumente* genannt.

Eine Funktion $f : A \to B$ heißt *injektiv*, falls verschiedene Elemente aus A auf verschiedene Elemente aus B abgebildet werden, d.h., aus $a, a' \in A, a \neq a'$ folgt $f(a) \neq f(a')$, f heißt *surjektiv*, falls es für jedes $b \in B$ ein $a \in A$ gibt, so dass $b = f(a)$, und f heißt *bijektiv*, falls f sowohl injektiv als auch surjektiv ist.

Binäre Relationen

Eine binäre Relation $R \subseteq A \times A$ heißt *reflexiv*, falls $(a,a) \in R$ für alle $a \in A$,

R heißt *symmetrisch* falls aus $(a,b) \in R$ folgt, dass $(b,a) \in R$,

R heißt *transitiv* falls aus $(a,b),(b,c) \in R$ folgt, dass auch $(a,c) \in R$,

und R heißt *antisymmetrisch*, falls aus $(a,b) \in R, a \neq b$ folgt, dass $(b,a) \notin R$.

Eine binäre Relation, die reflexiv, transitiv und symmetrisch ist, heißt *Äquivalenzrelation*.

Sei $R \subseteq A \times A$ eine Äquivalenzrelation.

$$[a]_R = \{b \mid (a,b) \in R\}$$

heißt die *Äquivalenzklasse* von a bezüglich R.

Satz:
Die Äquivalenzklassen einer Äquivalenzrelation $R \subseteq A \times A$ bilden eine Partition von A.

Eine binäre Relation $R \subseteq A \times A$, die reflexiv, transitiv und antisymmetrisch ist, heißt *partielle Ordnung* oder auch *Halbordnung* auf A. Sie heißt *totale Ordnung*, wenn für alle $a, b \in A, a \neq b$, entweder $(a,b) \in R$ oder $(b,a) \in R$.

Die *inverse Relation* einer binären Relation $R \subseteq A \times B$ ist die Relation

$$R^{-1} = \{(b,a) \mid (a,b) \in R\}$$

Ein *Pfad* in einer binären Relation $R \subseteq A \times A$ ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $(a_i, a_{i+1}) \in R$ für alle $i = 1, \ldots, n-1$. Ein Pfad heißt *einfacher Pfad*, falls alle a_i verschieden sind. Ein Pfad $(a_1, a_2, \ldots, a_n)$ hat *Länge* $n-1$.

Ein *Kreis* in einer binären Relation $R \subseteq A \times A$ ist eine Folge $(a_1, a_2, \ldots, a_n)$ für ein $n \geq 1$, so dass $(a_i, a_{i+1}) \in R$ für alle $i = 1, \ldots, n-1$ und ferner $(a_n, a_1) \in R$. Ein Kreis heißt *einfacher Kreis*, falls alle a_i verschieden sind. Ein Kreis $(a_1, a_2, \ldots, a_n)$ hat *Länge* n.

Sei $R \subseteq V \times V$ eine binäre Relation.

Die *reflexive Hülle* von R ist die Relation

$$R \cup \{(a,a) \mid a \in V\}$$

Die *transitive Hülle* von R ist die Relation

$$R \cup \{(a,b) \mid a,b \in V \text{ und es gibt einen Pfad positiver Länge von } a \text{ nach } b \text{ in } R\}$$

Die *reflexive, transitive Hülle* von R ist die Relation

$$R^* = \{(a,b) \mid a,b \in V \text{ und es gibt Pfad von } a \text{ nach } b \text{ in } R\}$$

Natürliche Bijektionen

Bestimmte Bijektionen, die besonders einfach sind, nennen wir natürliche Bijektionen.

Beispiele:

$$\phi : \mathbb{N} = \{1, 2, \ldots\} \to \{\{n\} \mid n \in \mathbb{N}\}$$

$$\phi(k) = \{k\}$$

$$\phi : A \times B \times C \to (A \times B) \times C$$

$$\phi(a,b,c) = ((a,b),c)$$

$$\phi : 2^{A \times B} \to \{f \mid f \text{ ist eine Funktion von } A \text{ nach } 2^B\}$$

$$\phi(R) = f : A \to 2^B, \text{ wobei}$$

$$f(a) = \{b \mid b \in B \text{ und } (a,b) \in R\}$$