Begründer der Berechenbarkeitstheorie

Alan Turing (1912–1954)

Alonzo Church (1903–1995)

Kurt Gödel (1906–1978)

Stephen Kleene (1909–1994)

Berechenbarkeit & Berechnungsmodelle

Algorithmus/Berechnung:

Zeichenmanipulation über endlichem Alphabet $\mathbb{A}$;

$\emptyset \neq \mathbb{A}$ endliches Alphabet

$\mathbb{A}^*$ Menge aller Wörter über $\mathbb{A}$ (abz. unendl.)
Datenmaterial für input/output/Zwischenschritte

zu berechnen: (partielle) Funktionen $f : \mathbb{A}^* \xrightarrow{\text{part}} \mathbb{A}^*$

konstitutiv: einfache, lokale Elementar-Operationen
Zeichenmanipulation an Wörtern in $\mathbb{A}^*$,
regelhafte, uniforme Ablauf-Steuerung

Modelle für prinzipielle Berechenbarkeit:
u.a. Turingmaschinen, Registermaschinen, μ-rekursive Funktionen

Turingmaschinen

Speichermedium: Band ($\mathbb{Z}$-indizierte Folge von Band-Zellen)
Bandzelle enthält $a \in \mathbb{A}$ oder ist leer ($\square$)

Zugriff: Lese-/Schreibkopf liest/überschreibt Zeichen

Steuerung: endliche Zustandsmenge Q und Übergangsfunktion
$\delta\colon Q \times (\mathbb{A} \cup \{\square\}) \to (\mathbb{A} \cup \{\square\}) \times \{-1, 0, 1\} \times Q$

Zustand $q \in Q$ und gelesenes Zeichen bestimmen
Schreibaktion, Kopfbewegung, Nachfolgezustand

Berechnung/Lauf auf Eingabewort w $\in \mathbb{A}^*$:
Übergangsregeln generieren Konfigurationsfolge
aus Startkonfiguration (Eingabewort/Startzustand/-position)
bis ggf. ein Haltezustand (und Ausgabewort) erreicht wird

Registermaschinen

Speichermedium: endliche Folge von Registern R_i
Register enthalten Wörter $w \in \mathbb{A}^*$

Zugriff: Anfügen/Löschen eines Zeichens $a \in \mathbb{A}$
am Ende des Worts in Register R_i
(und Abfrage des letzten Buchstabens)

Steuerung: Programmzeilen mit Verzweigungsbefehlen
anhand des letzten Buchstabens in R_i

Berechnung: Instruktionen generieren Konfigurationsfolge
aus Startkonfiguration (Eingabewörter/Startzeile)
bis ggf. ein Haltebefehl ausgeführt wird

die berechnete partielle Funktion

der Lauf der Register- oder Turingmaschine $\mathcal{M}$
auf Eingabewort $w \in \mathbb{A}^*$ kann *terminieren* oder *divergieren*

$w \xrightarrow{\mathcal{M}} \infty$ (divergent) oder $w \xrightarrow{\mathcal{M}} \mathrm{STOP}$

$w \xrightarrow{\mathcal{M}} w'$ (Ausgabe $w' \in \mathbb{A}^*$)

$w \xrightarrow{\mathcal{M}} q^{\pm}$ (boolesche Ausgabe)

die von $\mathcal{M}$ berechnete partielle Funktion $f_{\mathcal{M}}$ auf $\mathbb{A}^*$
hat Definitionsbereich $\{w \in \mathbb{A}^* : w \xrightarrow{\mathcal{M}} \mathrm{STOP}\} \subseteq \mathbb{A}^*$

Church–Turing These

empirisches Faktum: alle intuitiv (oder praktisch) berechenbaren Funktionen sind durch Turing- und Registermaschinen berechenbar

mathematisches Faktum: diverse Berechnungsmodelle (wie Turing- und Registermaschinen) und alternative Formalismen (wie μ-rekursive Funktionen) liefern denselben Begriff berechenbarer partieller Funktionen

Curch-Turing-These:
Turing-Berechenbarkeit = prinzipielle Berechenbarkeit

Grundbegriffe

Berechenbarkeit: (s.o.)

zB.: alle vertrauten arithmetischen Funktionen über $\mathbb{N}$

Entscheidbarkeit: $R \subseteq \mathbb{A}^*$ entscheidbar gdw.
die (totale) charakteristische Funktion $\chi_R : \mathbb{A}^* \to \mathbb{B}$ berechenbar

zB.: die Menge der Primzahlen
die Menge der erfüllbaren AL-Formeln
die Menge der allgemeingültigen AL-Formeln

Aufzählbarkeit: $R \subseteq \mathbb{A}^*$ aufzählbar gdw.
$R = \mathrm{Def}(f)$ für eine berechenbare partielle Funktion $f : \mathbb{A}^* \to \mathbb{A}^*$
(für $R \neq \emptyset$ äq.: $R = \mathrm{Bild}(f)$ für ein berechenbares totales $f : \mathbb{A}^* \to \mathbb{A}^*$)

zB.: die Menge der allgemeingültigen $\mathrm{FO}(\sigma_{ar})$-Formeln
die Menge der $\mathrm{FO}(\sigma_{ar})$-Formeln mit endlichen Modellen

Grenzen

- fast alle Funktionen $\mathbb{N} \to \mathbb{N}$ sind *nicht* berechenbar
- fast alle Teilmengen $S \subseteq \mathbb{N}$ sind *nicht* entscheidbar/aufzählbar

schwerer:
Nachweis der Unentscheidbarkeit einer konkreten Menge
(und hierfür Präzisierung des Berechnungsmodells notwendig)

Turing: Unentscheidbarkeit des Halteproblems

klassischer Diagonalisierungsbeweis

daraus durch Reduktion Unentscheidbarkeit vieler
relevanter Probleme aus Arithmetik, Kombinatorik, Logik, ...

Turing 1936: On Computable Numbers, with an Application to the Entscheidungsproblem

zur Unentscheidbarkeit des Halteproblems

Scooping the Loop Snooper

Geoffrey K. Pullum, 2008

No general procedure for bug checks will do.
Now, I won't just assert that, I'll prove it to you.
I will prove that although you might work till you drop,
you cannot tell if computation will stop.

For imagine we have a procedure called *P*
that for specified input permits you to see
whether specified source code, with all of its faults,
defines a routine that eventually halts.

...

Geoffrey K. Pullum, 2008
`www.lel.ed.ac.uk/~gpullum/loopsnoop.html`

Unentscheidbarkeitsresulate: Beispiele

unentscheidbar sind:

- die Menge der erfüllbaren $\mathrm{FO}(\sigma_{ar})$-Formeln
- die Menge der im Endlichen allgemeingültigen $\mathrm{FO}(\sigma_{ar})$-Formeln
- die Menge der in $\mathcal{N} = (\mathbb{N}, +, \cdot, 0, 1, <)$ wahren $\mathrm{FO}(\sigma_{ar})$-Formeln
  d.h. die FO-Theorie der Arithmetik über $\mathbb{N}$
- die FO-Theorien der Gruppen und der Graphen
- das Parkettierungsproblem

entscheidbar sind:

- die FO-Theorie der Arithmetik über $\mathbb{R}$
- die FO-Theorie der abelschen Gruppen

Errungenschaften

- innermathematische Konzepte von Logik & Semantik
- mathematischer Begriff des Algorithmus: Berechenbarkeit
- Gödelscher Vollständigkeitssatz für FO
  $\rightarrow$ prinzipielle Beweisbarkeit und Aufzählbarkeit
- FO-Axiomatisierung der Mathematik im Rahmen von ZFC

und prinzipielle Grenzen (besondere Errungenschaften)

- Unentscheidbarkeitsbeweise
- Unvollständigkeit von aufzählbaren Axiomatisierungen:
  1. Gödelscher Unvollständigkeitssatz
- Unbeweisbarkeit der Konsistenz von Axiomatisierungen:
  2. Gödelscher Unvollständigkeitssatz