Theoretische Informatik II

Einheit 7

Elementare Berechenbarkeitstheorie

1. Aufzählbarkeit und Entscheidbarkeit
2. Universelle Maschinen
3. Beweistechniken
4. Grenzen der Berechenbarkeit

Untersuchung von Fragen der Berechenbarkeit unabhängig vom Modell

- **Was kann überhaupt berechnet werden?**
  - Welche Funktionen sind berechenbar?
  - Welche Programmeigenschaften kann man entscheiden (testen)?
- **Wie kann man Lösungen wiederverwenden?**
  - Verwendung von Abschlußeigenschaften
  - Transformation in ein anderes Problem (Reduktion)
- **Wo liegen die Grenzen?**
  - Terminierung, Korrektheit, Äquivalenz, Optimalität von Programmen
- **Welche Beweistechniken gibt es?**
  - Konstruktion von abstrakten Gegenbeispielen durch Diagonalisierung
  - Problemreduktion
  - Direkte Beweise (Busy Beaver)

Berechenbarkeitstheorie – Vorgehensweise

- **Konzepte modellunabhängig präzisieren**
  - Berechenbare Funktionen
  - (Semi-)entscheidbare und aufzählbare Mengen
- **Grundeigenschaften aus Modellen herleiten**
  - Zusammenhänge zwischen den Konzepten
  - Abschlußeigenschaften
  - Codierung von Programmen als Daten
  - Existenz universeller Funktionen
- **Theorie nur auf dieser Basis weiterführen**
  - Hier: die wichtigsten Unmöglichkeitsaussagen

Theoretische Informatik II

Einheit 7.1

Aufzählbarkeit und Entscheidbarkeit

1. Präzisierung der Begriffe
2. Zusammenhänge
3. Abschlußeigenschaften

BERECHENBARKEIT

- **Berechenbarkeit auf Worten**
  - $f{:}X^*{\to}Y^*$ berechenbar, falls f Turing-berechenbar $\boxed{\text{Def. E, Kapitel 6}}$
- **Berechenbarkeit auf Wort-Tupeln $f{:}X^*{\times}X^*{\to}Y^*$**
  - $f{:}X^*{\times}X^*{\to}Y^*$ berechenbar, falls $f'{:}(X{\cup}\{\#\})^*{\to}Y^*$ mit $f'(v\#w) = f(v,w)$ berechenbar
- **Berechenbarkeit auf Zahlen**
  - $f{:}\mathbb{N}{\to}\mathbb{N}$ berechenbar, falls $f_r{:}X^*{\to}X^*$ mit $f_r(w) = r(f(\mathrm{r}^{-1}(w)))$ berechenbar
  - $r{:}\mathbb{N}{\to}X^*$ bijektive Repräsentation von Zahlen als Worte
- **Berechenbarkeit auf Zahlentupeln und -listen**
  - $f{:}\mathbb{N}^k{\to}\mathbb{N}$ berechenbar, falls $f'{:}\mathbb{N}{\to}\mathbb{N}$ mit $f'\langle x_1, x_2, .., x_k\rangle^k = f(x_1, x_2, .., x_k)$ berechenbar
  - $f{:}\mathbb{N}^*{\to}\mathbb{N}$ berechenbar, falls $f'{:}\mathbb{N}{\to}\mathbb{N}$ mit $f'\langle x_1, x_2, .., x_k\rangle^* = f(x_1 x_2 ... x_k)$ berechenbar
  - $\langle\rangle^k{:}\mathbb{N}^k{\to}\mathbb{N}$, $\langle\rangle^*{:}\mathbb{N}^*{\to}\mathbb{N}$ Standard-Tupelfunktionen $\boxed{\text{Kapitel 6.3}}$

Aufzählbarkeit und Entscheidbarkeit – intuitiv

- **Entscheidbarkeit einer Menge**
  – Wir können eine Maschine konstruieren, die testet, ob ein bestimmtes Element zur Menge gehört oder nicht
- **Semi-Entscheidbarkeit einer Menge**
  – Wir können eine Maschine konstruieren, die testet, ob ein bestimmtes Element zur Menge gehört, aber im Mißerfolgsfall eventuell niemals eine Antwort gibt
- **Aufzählbarkeit einer Menge**
  – Wir können eine Maschine konstruieren, welche die Elemente der Menge schrittweise generiert, also z.B. bei Eingabe der Zahl n (oder einer Codierung) das n-te Element der Menge ausgibt

Aufzählbarkeit und Entscheidbarkeit – präzisiert

- $M \subseteq X^*$ **entscheidbar** $\boxed{\text{Definition C}}$
  - $\chi_M : X^* \to \{0,1\}^*$ berechenbar, wobei $\chi_M(w) = \begin{cases} 1 & \text{falls } w \in M, \\ 0 & \text{sonst} \end{cases}$
- $M \subseteq X^*$ **semi-entscheidbar**
  - $\psi_M : X^* \to \{0,1\}^*$ berechenbar, wobei $\psi_M(w) = \begin{cases} 1 & \text{falls } w \in M, \\ \perp & \text{sonst} \end{cases}$
- $M \subseteq X^*$ **(rekursiv) aufzählbar** $\boxed{\text{Definition A}}$
  - $M = \emptyset$ oder es gibt eine totale, berechenbare Funktion $f : \{1\}^* \to X^*$
    mit $M = \text{range}(f) = \{v \in X^* \mid \exists w \in \{1\}^* \; f(w) = v\}$

- **Berechenbarkeit von Mengen** $M \subseteq \mathbb{N}$
  - M entscheidbar $\equiv$ $\chi_M : \mathbb{N} \to \mathbb{N}$ berechenbar
  - M semi-entscheidbar $\equiv$ $\psi_M : \mathbb{N} \to \mathbb{N}$ berechenbar

    wobei $\psi_M(n) = \begin{cases} 1 & \text{falls } n \in M, \\ \perp & \text{sonst} \end{cases}$ $\quad \chi_M(n) = \begin{cases} 1 & \text{falls } n \in M, \\ 0 & \text{sonst} \end{cases}$
  - M (rekursiv) aufzählbar $\equiv$ $M = \emptyset$ oder es gibt eine totale, berechenbare
    Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $M = \text{range}(f) = \{n \in \mathbb{N} \mid \exists i \in \mathbb{N} \; f(i) = n\}$

Aufzählbarkeit – Anmerkungen

- **Jede endliche Menge ist aufzählbar**
  - $M = \{x_0, ..., x_n\}$ ist Wertebereich von f mit $f(n) = \begin{cases} x_i & \text{falls } i{\leq}n, \\ x_0 & \text{sonst} \end{cases}$
  - f ist primitiv rekursiv, also berechenbar
- **Aufzählungen sind nicht notwendigerweise injektiv**
  - Die Funktion g mit $g(n) = \begin{cases} n{+}1 & \text{falls } n \text{ gerade,} \\ n & \text{sonst} \end{cases}$

    zählt alle ungeraden Zahlen genau zweimal auf
- **Jede Menge hat verschiedene Aufzählungen**
  - Die Funktion h mit $h(n) = 2n{+}1$

    zählt alle ungeraden Zahlen genau einmal auf
- **Es gibt viele äquivalente Charakterisierungen**
  - Aufzählbar — semi-entscheidbar — Typ-0 Sprache
  - Werte- oder Haltebereich einer (evtl. partiellen) berechenbaren Funktion

Charakterisierungen von Aufzählbarkeit

Satz B

Für $M\subseteq\mathbb{N}$ sind folgende Aussagen äquivalent

1. **M ist aufzählbar**
2. **M = range(f) für ein berechenbares f:$\mathbb{N}\to\mathbb{N}$**
   – $\mathrm{range}(f) = \{f(i) \mid i\in\mathbb{N}\}$, $\quad f$ nicht notwendigerweise total
3. **$\hat{M}$ ist Typ-0 Sprache**
   – wobei $\hat{M} = \{r(i) \mid i\in M\}$ für eine bijektive Repräsentation $r{:}\mathbb{N}\to X^*$
4. **M ist semi-entscheidbar**
5. **M = domain(f) für ein berechenbares f:$\mathbb{N}\to\mathbb{N}$**
   – $\mathrm{domain}(f) = \{i\in\mathbb{N} \mid f(i)\neq\perp\}$

Aussage gilt analog für $M\subseteq X^*$, $M\subseteq\mathbb{N}^k$, ...

Beweis der Äquivalenz durch Ringschluss

- **M aufzählbar $\Rightarrow$ M=range(f) für ein berechenbares f**
  - Es sei M aufzählbar
  - Falls M=$\emptyset$ dann ist M = range($f_\perp$), wobei $f_\perp(i) = \perp$ für alle $i \in \mathbb{N}$ $\surd$
  - Andernfalls M = range(f) für ein berechenbares, totales f $\surd$
- **M=range(f) für ein berechenbares f $\Rightarrow$ $\hat{M}$ Typ-0 Sprache**
  - Es sei M=range(f) für ein berechenbares f
  - Dann ist f Typ-0 berechenbar $\boxed{\text{Satz Q, Kap. 6}}$
  - Also $L_f = \{r(i)\#r(j)|f(i){=}j\}$ Typ-0 Sprache, d.h. $L_f = L(G)$ für ein G
  - Erweitere G zu Grammatik G', die zum Schluß alle Anteile $v\#$ entfernt
  - Dann ist $\hat{M} = \{r(j)\,|\,j \in M\} = \{r(j)\,|\,\exists i \in \mathbb{N} f(i)(=)j\} = L(G')$ $\surd$
- **$\hat{M}$ Typ-0 Sprache $\Rightarrow$ M semi-entscheidbar**
  - Unmittelbare Konsequenz von Satz Q, Kapitel 6 $\surd$
- **M semi-entscheidbar $\Rightarrow$ M=domain(f) für ein berechenbares f**
  - Es sei M semi-entscheidbar.
  - Dann ist ψ_M berechenbar und M=$\{i \in \mathbb{N}\,|\,\psi_M(i) = 1\}$ = domain(ψ_M) $\surd$

Beweis der Äquivalenz durch Ringschluss (II)

- **M=domain(f) für ein berechenbares $f \;\Rightarrow\; M$ aufzählbar**
  - Es sei $M = \text{domain}(f) = \{i \in \mathbb{N} \mid f(i) \neq \perp\}$ für ein berechenbares f
  - Falls $M = \emptyset$, dann ist M per Definition aufzählbar $\surd$
  - Andernfalls gibt es ein $n_0 \in \mathbb{N}$ mit $f(n_0) \neq \perp$ und eine TM τ mit $f = h_\tau$
  - Wir konstruieren eine Turingmaschine τ' mit $M = \text{range}(h_{\tau'})$

    Bei Eingabe einer (Repräsentation der) Zahl n arbeite τ' wie folgt

    1. Berechne i, j so daß $n = \langle i, j\rangle$
    2. Simuliere die Berechnung von τ bei Eingabe i für (maximal) j Schritte

       (Erzeuge Anfangskonfiguration, simuliere $\hat{\delta}_\tau$ auf separatem Band)
    3. Falls τ in j Schritten anhält, gebe i aus. Andernfalls gebe n_0 aus
  - τ' hält auf jeder Eingabe, also ist $h_{\tau'}$ total
  - $M \subseteq \text{range}(h_{\tau'})$: Sei $i \in M$. Dann gibt es ein j so daß τ nach j Schritten hält.

    Damit $h_{\tau'}(\langle i, j\rangle) = i$, also $i \in \text{range}(h_{\tau'})$
  - $M \supseteq \text{range}(h_{\tau'})$: Sei $i \in \text{range}(h_{\tau'})$. Falls $i = n_0$ dann $i \in M$ nach Voraussetzung.

    Andernfalls gibt es ein j so daß τ nach j Schritten hält.

    Also $i \in \text{domain}(h_\tau) = M$. $\surd$

Beispiele entscheidbarer / aufzählbarer Mengen

Sei f:ℕ→ℕ total berechenbar, g:ℕ→ℕ berechenbar

- **graph(f) $= \{(i,j) \mid f(i) = j\}$ ist entscheidbar**
  - Bei Eingabe (i,j) berechne $f(i)$ (hält immer) und vergleiche mit j
- **range(f) $= \{j \mid \exists i \in \mathbb{N}\, f(i) = j\}$ ist aufzählbar**
  - Charakterisierung #2
- **range(g) $= \{j \mid \exists i \in \mathbb{N}\, g(i) = j\}$ ist aufzählbar**
  - Charakterisierung #2
- **graph(g) $= \{(i,j) \mid g(i) = j\}$ ist aufzählbar**
  - Bei Eingabe (i,j) berechne $g(i)$ (hält nicht immer) und vergleiche
- **domain(g) $= \{i \mid g(i)\text{hält}\}$ ist aufzählbar**
  - Charakterisierung #5

Aufzählbarkeit vs. Entscheidbarkeit

$M \subseteq \mathbb{N}$ entscheidbar $\Leftrightarrow$ M und $\overline{M}$ aufzählbar Satz D

$\Rightarrow$ Es sei M entscheidbar. Dann ist $\chi_M{:}\mathbb{N}\to\mathbb{N}$ berechenbar.

Es ist $\psi_M(n) = \begin{cases} 1 & \text{falls } \chi_M(n)=1, \\ \perp & \text{sonst} \end{cases}$ und $\psi_{\overline{M}}(n) = \begin{cases} 1 & \text{falls } \chi_M(n)=0, \\ \perp & \text{sonst} \end{cases}$

Damit sind ψ_M und $\psi_{\overline{M}}$ berechenbar, also M und $\overline{M}$ aufzählbar ✓

$\Leftarrow$ Seien M und $\overline{M}$ aufzählbar.

Falls $M=\emptyset$ oder $\overline{M}=\emptyset$, so ist M trivialerweise entscheidbar ✓

Andernfalls $M=\text{range}(f)$ und $\overline{M}=\text{range}(g)$ wobei f, g total berechenbar.

Wir konstruieren eine Turingmaschine τ mit $\chi_M=h_\tau$

– Bei Eingabe von n berechne $j = \min\{i \mid f(i)=n \,\vee\, f(i)=n\}$

– Falls $f(j)=n$, gebe 1 aus, ansonsten 0

τ hält für jedes n, da $n \in \text{range}(f)$ oder $n \in \text{range}(g)$ $(n \in M \;/\; n \notin M)$

Für $n \in M$ gilt $f(j)=n$ für ein j, also $h_\tau(n)=1$, ansonsten $h_\tau(n)=0$ ✓

Aufzählbarkeit vs. Entscheidbarkeit

- **Jede entscheidbare Menge ist aufzählbar**
  - Die Umkehrung gilt nicht (Beispiel folgt später)
- **Ist M endlich, so ist M entscheidbar und aufzählbar**
  - Für $M = \{x_1, ..., x_n\}$ ist $\chi_M(n) = \begin{cases} 1 & n{=}x_1 \vee \ldots \vee n{=}x_n\ , \\ 0 & \text{sonst} \end{cases}$
  - χ_M ist berechenbar, also ist M entscheidbar ✓
- **$M{\subseteq}\mathbb{N}$ aufzählbar $\Leftrightarrow$ es gibt ein entscheidbares $M'{\subseteq}\mathbb{N}\times\mathbb{N}$**
  mit $M = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N}\ (n, y) \in M'\}$

  $\Rightarrow$: Es sei $M{\subseteq}\mathbb{N}$ aufzählbar
  - Falls $M{=}\emptyset$, so ist $M = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N}\ (n, y) \in \emptyset\}$ ✓
  - Andernfalls ist $M{=}\text{range}(f)$ für ein berechenbares, totales f
    und $\text{range}(f) = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N}\ (n, y) \in \text{graph}(f)\}$ ✓

  $\Leftarrow$: Es sei $M = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N}\ (n, y) \in M'\}$ für ein entscheidbares M'
  - Dann ist $\psi_M(y) = \text{sign}\ (\min\{n \in \mathbb{N} \mid (n, y) \in M'\})$
    $= \text{sign}\ (\min\{n \in \mathbb{N} \mid \chi_{M'}(n, y){=}1\})$ ✓

ABSCHLUSSEIGENSCHAFTEN

Satz E

Sei M, $M' \subseteq X^*$, f berechenbar und total, g berechenbar

- **Sind M, M' aufzählbar, dann auch**

  $M \cup M'$, $M \cap M'$, $M \circ M'$, M^*, $g(M)$, $g^{-1}(M)$

  Vereinigung, Durchschnitt, Konkatenation, Konkatenationsabschluß, Urbild

  Abschluß unter Komplement oder Differenz gilt nicht

- **Sind M, M' entscheidbar, dann auch**

  $M \cup M'$, $M \cap M'$, $M \backslash M'$, $\overline{M}$, $M \circ M'$, M^*, $f^{-1}(M)$

  Vereinigung, Durchschnitt, Differenz, Komplement, Konkatenation, -abschluß, Urbild

Aussage gilt analog für Teilmengen von $\mathbb{N}$, $\mathbb{N}^k$, ...

$\overline{M} = \{w \in X^* \mid w \notin M\}$ $\quad$ $M \circ M' = \{wv \mid w \in M \wedge v \in M'\}$ $\quad$ $M^* = \{w_1..w_n \mid w_i \in M\}$

$f^{-1}(M) = \{w \in X^* \mid f(w) \in M\}$ $\quad$ $f(M) = \{f(w) \mid w \in M\}$

Beweis der Abschlusseigenschaften

- Es seien M, M' aufzählbar mit Funktionen f und f'

  $\boldsymbol{M\cup M'}$: Für $h(w) = \begin{cases} f(v) & \text{falls } w{=}0v, \\ f'(v) & \text{falls } w{=}1v \end{cases}$ ist $\text{range}(h) = M\cup M'$

  $\boldsymbol{M\cap M'}$: $\psi_{M\cap M'}(w) = \psi_M(w) * \psi_{M'}(w)$

  $\boldsymbol{M\circ M'}$: Für $h(w\#v) = f(w)\circ f'(v)$ ist $\text{range}(h) = M\circ M'$

  $\boldsymbol{M^*}$: Für $h(w_1\#\ldots\#w_n) = f(w_1)\circ\ldots\circ f(w_n)$ ist $\text{range}(h) = M^*$

  $\boldsymbol{g(M)}$: Für $h(w) = g(f(w))$ ist $\text{range}(h) = g(M)$

  $\boldsymbol{g^{-1}(M)}$: $\psi_{g^{-1}(M)}(w) = \psi_M(g(w))$

  Details in Übungen präzisieren

- Entscheidbare Mengen sind abgeschlossen unter $\cup$, $\cap$, $\setminus$, $\bar{\ }$, $\circ$, *, f^{-1}

  Beweis in Übungen