Theoretische Informatik II

Einheit 5.4

Elementare Berechenbarkeitstheorie I:

Grundkonzepte und ihre Eigenschaften

1. Grundgesetze der Berechenbarkeit
2. Berechenbarkeit, Aufzählbarkeit
   und Entscheidbarkeit
3. Abschlußeigenschaften

ELEMENTARE BERECHENBARKEITSTHEORIE

- **Es gibt viele Fragen zur Berechenbarkeit**
  - Welche Funktionen sind berechenbar und welche nicht?
  - Welche Probleme sind (semi-)entscheidbar und welche nicht?
  - Abschlußeigenschaften: wie kann man Lösungen wiederverwenden?
  - Grenzen des Machbaren: was ist nicht mehr berechenbar?
    Wie kann man nachweisen, daß ein Problem nicht lösbar ist?
- **Antworten hängen nicht vom Berechnungsmodell ab**
  - Berechenbarkeit, (semi-)Entscheidbarkeit, (Zeit-/Platz)Komplexität
    sind allgemeine Konzepte
- **Löse Theorie von Betrachtung konkreter Modelle**
  - Formuliere Grundeigenschaften (Axiome) berechenbarer Funktionen
  - Beweise diese Eigenschaften mit einem Modell (Turingmaschine)
  - Stütze alle Beweise für Aussagen nur noch auf diese Eigenschaften
    denn sie gelten für alle gleichmächtigen Berechnungsmodelle

Formuliere Theorie berechenbarer Funktionen

- **Es reicht berechenbare Funktionen zu betrachten**
  - (Semi-)Entscheidbarkeit einer Menge ist äquivalent zur Berechenbarkeit ihrer (partiell-)charakteristischen Funktion
- **Es reicht Berechenbarkeit auf Zahlen zu betrachten**
  - Berechenbarkeitskonzepte auf Wörtern und Zahlen sind gleichwertig
    - · Zahlen kann man als Wörter (binär oder anders) codieren
    - · Wörter über einem Alphabet kann man systematisch numerieren
  - Es ist meist leichter, mit Zahlen zu arbeiten (z.B. Rechenzeit)
  - Programme und Daten sind als Zahlen codierbar
- **Es reicht einstellige Funktionen auf $\mathbb{N}\to\mathbb{N}$ zu betrachten**
  - Funktionen auf Zahlenpaaren und -listen sind einstellig simulierbar

    z.B. ist $f{:}\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ durch $f'{:}\mathbb{N}\to\mathbb{N}$ mit $f'\langle i,j\rangle := f(i,j)$ simulierbar

Liefert allgemeine Theorie der Berechenbarkeit

Berechenbare Funktionen lassen sich aufzählen

- **Turingmaschinen sind als Wörter codierbar**
  - Es reicht, Turingmaschinen mit Γ=$\{0, 1, B\}$ und F=$\{q_1\}$ zu betrachten
  - Definiere code($\delta(q,X)$) $\equiv$ $q\,X\,p\,Y\,D$, falls $\delta(q,X)$=(p,Y,D)
  - Codiere die Maschine M = $(Q, \Sigma, \Gamma, \delta, q_0, B, F)$ durch das Wort

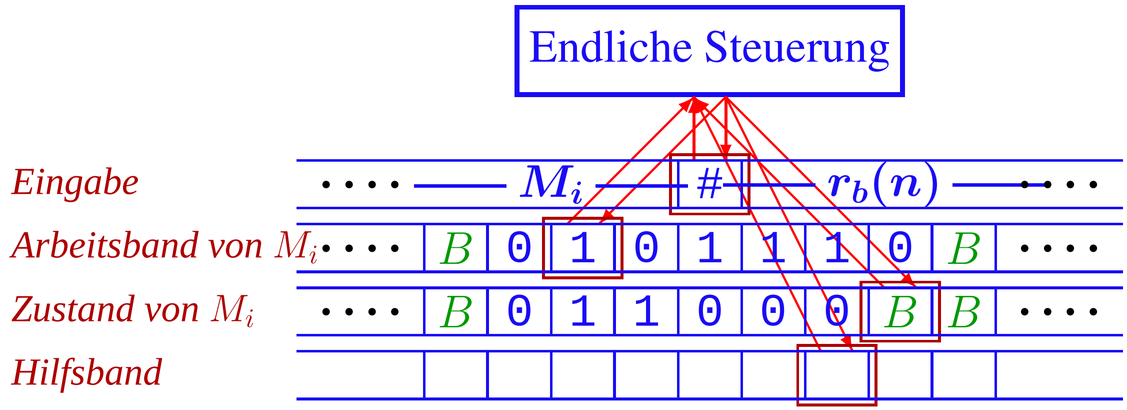
    code($\delta(q_0$,0))#code($\delta(q_0$,1))#code($\delta(q_0,B)$)#...#code($\delta(q_n,B)$)
  - Alphabet ist Δ = $\{q_0, .., q_n, 0, 1, B, L, R, \#\}$ (Binärcodierung auch möglich)
- **Wörter über einem Alphabet sind numerierbar**
  - Bestimme lexikographische Ordnung der Wörter über Δ = $\{x_1, .., x_n\}$

    $\epsilon < x_1 < \ldots < x_n < x_1x_1 < x_1x_2 < \ldots < x_nx_n < x_1x_1x_1 < \ldots$
  - Zähle entsprechend durch: w_0:=ϵ, w_1:=x_1, .. w_n:=x_n, w_{n+1}:=x_1x_1, ...
- **Turingmaschinen sind (bijektiv) numerierbar**
  - Zähle Wörter über Δ auf und teste, ob sie Turingmaschinen codieren
  - M_i ist die Turingmaschine, deren Codierung an i-ter Stelle erscheint
  - Die Nummer i wird auch die **Gödelnummer** von M_i genannt

Numerierung von TM liefert zwei Kernaxiome

- **Definiere Numerierung berechenbarer Funktionen:**
  - φ_i ist die von M_i berechnete (partielle) Funktion auf $\mathbb{N}$
    - $\varphi(i) := \varphi_i := r_b^{-1} \circ f_{M_i} \circ r_b$, wobei $r_b : \mathbb{N} \to \{0,1\}^*$ Binärcodierung von $\mathbb{N}$
  - Φ_i ist die zugehörige Schrittzahlfunktion von M_i
    - $\Phi(i)(n) := \Phi_i(n) := t_{M_i}(r_b(n))$
- **$\varphi : \mathbb{N} \to \mathcal{R}$ is surjektiv, aber nicht bijektiv**
  - Jede programmierbare Funktion hat einen Index
  - Jede berechenbare Funktion hat unendlich viele Programme
- Axiom 1: **Für alle i gilt domain(Φ_i)=domain(φ_i)**
  - Per Konstruktion ist Φ_i auf den gleichen Eingaben definiert wie φ_i
- Axiom 2: **$\{\langle i, n, t\rangle \mid \Phi_i(n) = t\}$ ist entscheidbar**
  - Simuliere Ausführung von $\varphi_i(n)$ für maximal t Schritte
  - Implementierung benutzt Variante der universellen Maschine (s.u.)

Axiom 3: Die universelle Funktion ist berechenbar



- **Benutze 3 Arbeitsbänder + Hilfsbänder**
  - Programmnummer i und Eingabewert n, binär codiert
  - Arbeitsband von M_i
  - Aktueller Zustand von M_i (auf Band, da Anzahl der Zustände nicht limitiert)
- **Generiere und simuliere Programm von M_i**
  - Generiere das Wort, das M_i über Δ codiert; schreibe es auf Band 1
  - Kopiere $r_b(n)$ auf Band 2 und schreibe q_0 auf Band 3
  - Simuliere Einzelschritte von M_i durch Aufsuchen der Befehle auf Band 1
  - Terminiert M_i (Zustand q_1), kopiere die Ausgabe von Band 2 auf Band 1

$u : \mathbb{N} \longrightarrow \mathbb{N}$ mit $u\langle i, n\rangle = \varphi_i(n)$ ist berechenbar (UTM Theorem)

Axiom 4: Programme sind effektiv kombinierbar

Es gibt eine berechenbare totale Funktion $s{:}\mathbb{N}\longrightarrow\mathbb{N}$ mit
$\varphi_{s\langle m,n\rangle}(i) = \varphi_m\langle n,i\rangle$ für alle $m,n,i\in\mathbb{N}$ (SMN Theorem)

- **Konstruiere eine Turingmaschine M für s:**
  - Auf dem Eingabeband stehe die Codierung einer Zahl $\langle m,n\rangle$
  - Konstruiere auf Hilfsband 1 die Codierung der m-ten Turingmaschine M_m
  - Konstruiere auf Hilfsband 2 die Codierung einer Maschine $M_{\langle\rangle}$, welche bei Eingabe einer Zahl i den Wert $f_{M_{\langle\rangle}}(i) = \langle n,i\rangle$ berechnet.
  - Konstruiere auf Hilfsband 3 den Code einer Maschine, die bei Eingabe einer Zahl i zunächst $M_{\langle\rangle}$ simuliert und M_m auf das Ergebnis anwendet.
  - Berechne die Gödelnummer der so aus $\langle m,n\rangle$ konstruierten Maschine
- **Setze $s := f_M$**
  - Per Konstruktion ist die Funktion s berechenbar
  - s ist total, weil M für jede Eingabe $\langle m,n\rangle$ ein Ergebnis produziert
  - Es gilt $\varphi_{s\langle m,n\rangle}(i) = f_{M_m}(f_{M_{\langle\rangle}}(i)) = \varphi_m\langle n,i\rangle$

Programme sind fast beliebig ineinander übersetzbar

- **Für jede berechenbare Funktion f gibt es ein $h \in \mathcal{TR}$ mit $\varphi_{h(n)}(i) = f\langle n, i\rangle$ für alle $n, i \in \mathbb{N}$**

  Beweis: wenn $f = \varphi_m$ ist, so wähle $h(n) := s\langle m, n\rangle$

- **Berechenbare Funktionen sind effektiv kombinierbar**

  Es gibt eine berechenbare totale Funktion h mit $\varphi_{h\langle i,j\rangle} = \varphi_i \circ \varphi_j$

  Intuitiv: h berechnet die Gödelnummer der Kombination von M_i und M_j

  Beweis: die Funktion f mit $f\langle\langle i, j\rangle, x\rangle := \varphi_i(\varphi_j(x))$ ist berechenbar

  Also gibt es ein $h \in \mathcal{TR}$ mit $\varphi_{h\langle i,j\rangle}(x) = f\langle\langle i, j\rangle, x\rangle = (\varphi_i \circ \varphi_j)(x)$

- **Es gibt berechenbare totale Funktionen f, g mit**
  - $\varphi_{f(i)}(n) = \varphi_i(n)+1$ für alle i, n
  - $\varphi_{g\langle i,j\rangle}(n) = \varphi_i(n)+\varphi_j(n)$ für alle i, j, n

  $\vdots$

Berechenbarkeitstheorie braucht nur vier Axiome

Berechenbare Funktionen sind effektiv numerierbar

Es gibt Funktionen φ:$\mathbb{N}\longrightarrow\mathcal{R}$ und Φ:$\mathbb{N}\longrightarrow\mathcal{R}$ mit

1. φ_i und Φ_i haben immer denselben Definitionsbereich

Intuition: $\varphi_i \hat{=} \varphi(i)$ ist die vom i-ten Programm berechnete Funktion

$\Phi_i \hat{=} \Phi(i)$ ist die zu φ_i gehörende Rechenzeitfunktion

2. Rechenzeit ist entscheidbar

– Man kann für beliebige $i, n, t \in \mathbb{N}$ testen ob $\Phi_i(n) = t$ ist oder nicht

3. Computer sind universelle Maschinen (UTM Theorem)

– Eine Maschine kann alle Programme und Daten verarbeiten

– Die Funktion u :$\mathbb{N}\rightarrow\mathbb{N}$ mit $u\langle i, n\rangle = \varphi_i(n)$ ist berechenbar

4. Programme sind effektiv kombinierbar (SMN Theorem)

– Die Nummer des entstehenden Programms kann berechnet werden

– Es gibt eine berechenbare totale Funktion s mit $\varphi_{s\langle m,n\rangle}(i) = \varphi_m\langle n, i\rangle$

ZENTRALE BERECHENBARKEITSKONZEPTE

- **Berechenbare Funktion $f : \mathbb{N}\longrightarrow\mathbb{N}$** ("$f$ ist **(partiell) rekursiv**")
  - Es gibt ein $i \in \mathbb{N}$ mit $f = \varphi_i$ (Es gibt ein Programm zur Berechnung von f)
  - f heißt **total rekursiv**, wenn f berechenbar und total ist
- **Entscheidbare Menge M** ('M ist **rekursiv**")

  Es gibt ein Programm, das testet, ob ein Element zu M gehört oder nicht
  - Die charakteristische Funktion χ_M ist berechenbar

  $$\boxed{\chi_M(x) = \begin{cases} 1 \text{ falls } x \in M, \\ 0 \text{ sonst} \end{cases}}$$
- **Semi-entscheidbare Menge M**

  Es gibt ein Programm, das testet, ob ein Element zu M gehört, aber nicht immer anhält
  - Die partielle charakteristische Funktion ψ_M ist berechenbar

  $$\boxed{\psi_M(x) = \begin{cases} 1 & \text{falls } x \in M, \\ \perp & \text{sonst} \end{cases}}$$
- **Neu: (rekursiv) aufzählbare Menge M**

  Es gibt ein Programm, das schrittweise alle Elemente von M generiert
  - $M{=}\emptyset$ oder es gibt eine totale, berechenbare Funktion f mit $M = \text{range}(f)$

  $$\boxed{\text{range}(f) = \{n \in \mathbb{N} \mid \exists i \in \mathbb{N}\ f(i){=}n\}}$$

Anmerkungen zur Aufzählbarkeit

- **Nicht identisch mit Abzählbarkeit**
  - M abzählbar, wenn es eine surjektive Funktion f von $\mathbb{N}$ nach M gibt
  - M aufzählbar, wenn M Bild einer berechenbaren Funktion ist
- **Aufzählungen müssen nicht injektiv sein**
  - 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**
  - $h = \lambda n.2n+1$ zählt alle ungeraden Zahlen genau einmal auf
- **Jede endliche Menge ist aufzählbar**
  - $M = \{x_0, .., x_n\}$ ist Bild 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

Es gibt viele äquivalente Charakterisierungen für rekursiv aufzählbare Mengen

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

1. **M ist aufzählbar**
2. **M = range(f) für ein berechenbares $f : \mathbb{N} \longrightarrow \mathbb{N}$**
   – **range(f)**= $\{f(i) \mid i \in \mathbb{N}\}$, f nicht notwendigerweise total
3. **M ist semi-entscheidbar**
4. **M = domain(f) für ein berechenbares $f : \mathbb{N} \longrightarrow \mathbb{N}$**
   – **domain(f)**= $\{i \in \mathbb{N} \mid f(i) \neq \perp\}$

Analog für Mengen über Worten, Zahlentupeln, . . .

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 $\Rightarrow$ M semi-entscheidbar**
  - Es sei M=range(f) für ein berechenbares, möglicherweise partielles f
  - Dann ist $m \in M$ genau dann, wenn m=$f(n)$ für ein $n \in \mathbb{N}$
  - Für $i \in \mathbb{N}$ mit f=φ_i ist $\psi_M(m)$ = sign (min$\{\langle n,t\rangle | \Phi_i(n){=}t \wedge \varphi_i(n){=}m\}$)

    Standardtrick: simultanes Durchzählen von Eingabewerten und Rechenzeitschranken
  - Da die Rechenzeitfunktion entscheidbar ist, ist ψ_M berechenbar $\surd$
- **M semi-entscheidbar $\Rightarrow$ M=domain(f) für ein berechenbares f**
  - Es sei M semi-entscheidbar.
  - Dann ist ψ_M berechenbar und M=$\{i \in \mathbb{N} \mid \psi_M(i) = 1\}$ = domain(ψ_M) $\surd$

Beweis der Äquivalenz durch Ringschluss (II)

- **M=domain(f) für ein berechenbares f $\Rightarrow$ M aufzählbar**
  - Es sei M = 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 $i \in \mathbb{N}$ mit $f = \varphi_i$ und ein $n_0 \in \mathbb{N}$ mit $f(n_0) \neq \perp$
  - Wir konstruieren eine berechenbare totale Funktion g mit M=range(g)

    Es sei $g\langle n,t\rangle = \begin{cases} n & \text{falls } \Phi_i(n)=t, \\ n_0 & \text{sonst} \end{cases}$

    Standardtrick: Zerlegen der Eingabe mit Umkehrfunktionen der Standardtupelfunktion
  - Da die Rechenzeitfunktion entscheidbar ist, ist g total und berechenbar
  - M=range(g): Es gilt $n \in M$=domain(φ_i)

    $\Leftrightarrow$ es gibt es eine Rechenzeit t mit $\Phi_i(n)=t$

    $\Leftrightarrow$ $g\langle n,t\rangle = n$

    $\Leftrightarrow$ $n \in$ range(g) $\surd$

Wichtige entscheidbare und aufzählbare Mengen

- **Sei f:$\mathbb{N}\longrightarrow\mathbb{N}$ berechenbar**
  - **range(f) ist aufzählbar** — Charakterisierung #2
  - **domain(f) ist aufzählbar** — Charakterisierung #4
  - **graph(f) ist aufzählbar (entscheidbar, wenn f total ist)**

    Bei Eingabe $\langle i,j\rangle$ teste $f(i)=j$ (hält immer, wenn f total)
- $\{\langle i,n,t\rangle \mid \Phi_i(n)=t\}$ **ist entscheidbar** — Axiom 2
- $\{\langle i,n,y\rangle \mid \varphi_i(n)=y\}$ **ist aufzählbar**
  - Graph der universellen Funktion
- $H = \{\langle i,n\rangle \mid n\in \mathbf{domain}(\varphi_i)\}$ **ist aufzählbar**
  - Definitionsbereich der universellen Funktion — (Halteproblem)
- $S = \{i \mid i\in \mathbf{domain}(\varphi_i)\}$ **ist aufzählbar**
  - Definitionsbereich von $\lambda i.u\langle i,i\rangle$ — (Selbstanwendbarkeitsproblem)

AUFZÄHLBARKEIT VS. ENTSCHEIDBARKEIT

M entscheidbar $\Leftrightarrow$ M und $\overline{M}$ aufzählbar

$\Rightarrow$ 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 $\surd$

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

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

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

Definiere $h{:}\mathbb{N}\to\mathbb{N}$ durch $h(n) = \min\{i \mid f(i){=}n \lor g(i){=}n\}$

Dann ist h berechenbar und total, da $n \in M$ oder $n \in \overline{M}$ für jedes n gilt.

Damit ist $\chi_M(n) = \begin{cases} 1 & \text{falls } f(h(n)) = n, \\ 0 & \text{sonst} \end{cases}$ berechenbar $\surd$

Aufzählbarkeit vs. Entscheidbarkeit II

- **Jede entscheidbare Menge ist aufzählbar**
  - Die Umkehrung gilt nicht (Beispiel folgt in §5.5)
- **Jede endliche Menge ist 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 $\surd$
- **M ist aufzählbar g.d.w. es eine entscheidbare Menge M' gibt mit $M = \{y \in \mathbb{N} \mid \exists n \in \mathbb{N}\ \langle n, y\rangle \in M'\}$** (Projektionssatz)

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

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

    $= \text{sign}\,(\min\{n \in \mathbb{N} \mid \chi_{M'}\langle n, y\rangle{=}1\}{+}1)$ berechenbar $\surd$

Aufzählbare Mengen sind abgeschlossen unter

- **$M \cup M'$: Vereinigung**
  - Seien M=range(h) und M'=range(h') aufzählbar
  - Definiere g durch $g(n) = \begin{cases} h(\lfloor n/2 \rfloor) & \text{falls } n \text{ gerade,} \\ h'(\lfloor n/2 \rfloor) & \text{sonst} \end{cases}$
  - Dann ist g berechenbar und range(g) = $M \cup M'$ aufzählbar
- **$M \cap M'$: Durchschnitt**
  - Es ist $\psi_{M \cap M'}(n) = \psi_M(n) * \psi_{M'}(n)$. Also ist $\psi_{M \cap M'}$ berechenbar

    In beiden Fällen erhalten wir eine 1 genau dann, wenn n $\in M \cap M'$
- **$f(M)$: Bild einer berechenbaren Funktion**
  - Definiere g durch $g(n) = f(h(n))$
  - Dann ist g berechenbar und range(g) = $f(M)$ aufzählbar
- **$f^{-1}(M)$: Urbild einer berechenbaren Funktion**
  - Es ist $\psi_{f^{-1}(M)}(n) = \psi_M(f(n))$. Also ist $\psi_{f^{-1}(M)}$ berechenbar.

Kein Abschluß unter Komplement oder Differenz

ABSCHLUSSEIGENSCHAFTEN ENTSCHEIDBARER MENGEN

Entscheidbare Mengen sind abgeschlossen unter

- $M \cup M'$: **Vereinigung**
  - Beweisidee: $\chi_{M \bigcup M'}(n) = \mathrm{sign}(\chi_M(n) + \chi_{M'}(n))$.
- $M \cap M'$: **Durchschnitt**
  - Beweisidee: $\chi_{M \bigcap M'}(n) = \chi_M(n) * \chi_{M'}(n)$.
- $\overline{M}$: **Komplement**
  - Beweisidee: $\chi_{\overline{M}}(n) = 1 - \chi_M(n)$.
- M-M': **Differenz**
  - Beweisidee: $M\text{-}M' = M \cap \overline{M'}$
- $f^{-1}(M)$: **Urbild einer berechenbaren totalen Funktion**
  - Beweisidee: $\chi_{f^{-1}(M)}(n) = \chi_M(f(n))$.

Kein Abschluß unter Bild berechenbarer Funktionen

Rückblick elementare Berechenbarkeitstheorie

- **Es gibt 3 Grundkonzepte der Berechenbarkeit**
  - Berechenbare Funktionen, entscheidbare und aufzählbare Mengen
  - Es gibt viele äquivalente Charakterisierungen

  Alle Konzepte sind beschreibbar durch berechenbare Funktionen auf $\mathbb{N}$
  - Aufzählbare Mengen sind abgeschlossen unter $\cup$, $\cap$, f, f^{-1}
  - Entscheidbare Mengen sind abgeschlossen unter $\cup$, $\cap$, , -, f^{-1}
- **Alle Theorie stützt sich auf nur vier Gesetze**
  1. Numerierbarkeit von berechenbaren Funktionen und Rechenzeiten
  2. Entscheidbarkeit der Rechenzeit
  3. Berechenbarkeit der universellen Funktion
  4. Effektive Kombinierbarkeit berechenbarer Funktionen

  Jedes Berechenbarkeitsmodell erfüllt diese Axiome

Mehr Details in Vossen & Witt §9 und den dort angegebenen Referenzen