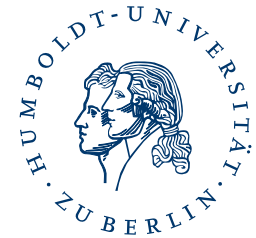
Einführung in die Theoretische Informatik

Johannes Köbler



Institut für Informatik
Humboldt-Universität zu Berlin

WS 2022/23

Entscheidbare und semi-entscheidbare Sprachen

Definition

- Eine NTM M hält bei Eingabe x (kurz: $M(x) = \downarrow$ oder $M(x)\downarrow$), falls alle Rechnungen von $M(x)$ nach endlich vielen Schritten halten
- Falls $M(x)$ nicht hält, schreiben wir auch kurz $M(x) = \uparrow$ oder $M(x)\uparrow$
- Eine NTM M entscheidet eine Eingabe x, falls $M(x)$ hält oder eine Konfiguration mit einem Endzustand erreicht
- Eine Sprache heißt entscheidbar, falls sie von einer DTM M akzeptiert wird, die alle Eingaben entscheidet. Die zugehörige Sprachklasse ist

$$\text{REC} = \{L(M) \mid M \text{ ist eine DTM, die alle Eingaben entscheidet}\}$$

- Jede von einer DTM akzeptierte Sprache heißt semi-entscheidbar

Bemerkung

- Eine DTM M entscheidet zwar immer alle Eingaben $x \in L(M)$, aber eventuell nicht alle $x \in \overline{L(M)}$. Daher heißt $L(M)$ semi-entscheidbar
- Später werden wir die Gleichheit $\text{RE} = \{L(M) \mid M \text{ ist eine DTM}\}$ zeigen

Berechnung von Funktionen

Definition

- Eine k-DTM $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ berechnet eine Funktion $f : \Sigma^* \to \Gamma^*$, falls M bei jeder Eingabe $x \in \Sigma^*$ in einer Konfiguration

  $$K = (q, u_1, a_1, v_1, \ldots, u_k, a_k, v_k) \text{ mit } u_k = f(x)$$

  hält (d.h. $K_x \vdash^* K$ und K hat keine Folgekonfiguration)
- Hierfür sagen wir auch, M gibt bei Eingabe x das Wort $f(x)$ aus und schreiben $M(x) = f(x)$
- f heißt Turing-berechenbar (oder einfach berechenbar), falls es eine k-DTM M mit $M(x) = f(x)$ für alle $x \in \Sigma^*$ gibt
- Aus historischen Gründen werden berechenbare Funktionen auch rekursiv (engl. *recursive*) genannt

Berechenbarkeit von charakteristischen Funktionen

Definition

Für eine Sprache $A \subseteq \Sigma^*$ ist die charakteristische Funktion $\chi_A : \Sigma^* \to \{0, 1\}$ wie folgt definiert:

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

Bemerkung

- In den Übungen wird gezeigt, dass eine Sprache A genau dann entscheidbar ist, wenn χ_A berechenbar (also rekursiv) ist
- Dies erklärt die Bezeichnung REC für die Klasse der entscheidbaren Sprachen
- Dort wird auch gezeigt, dass CSL echt in REC enthalten ist
- Beispiele für interessante semi-entscheidbare Sprachen, die nicht entscheidbar sind, werden wir später kennenlernen
- Somit gilt REG $\subsetneq$ DCFL $\subsetneq$ CFL $\subsetneq$ DCSL $\subseteq$ CSL $\subsetneq$ REC $\subsetneq$ RE

Berechenbarkeit von partiellen Funktionen

Definition

- Eine partielle Funktion hat die Form $f : A \to B \cup \{\uparrow\}$, wobei $\uparrow \notin B$ ist
- Für $f(x) = \uparrow$ sagen wir auch $f(x)$ ist undefiniert
- Der Definitionsbereich (engl. *domain*) von f ist

  $$dom(f) = \{x \in A \mid f(x) \neq \uparrow\}$$

- Das Bild (engl. *image*) von f ist

  $$img(f) = \{f(x) \mid x \in dom(f)\}$$

- Eine partielle Funktion $f : A \to B \cup \{\uparrow\}$ heißt total, falls $dom(f) = A$ ist
- Eine partielle Funktion $f : \Sigma^* \to \Gamma^* \cup \{\uparrow\}$ heißt berechenbar, falls es eine DTM $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ gibt, die f berechnet (d.h. $M(x)$ gibt für alle $x \in dom(f)$ das Wort $f(x)$ aus und hält im Fall $x \notin dom(f)$ nicht)
- In diesem Fall gilt also $M(x) = f(x)$ für alle $x \in \Sigma^*$ und wir bezeichnen die Menge $dom(f) = \{x \in \Sigma^* \mid M(x)\downarrow\}$ auch mit $dom(M)$

Definition (Fortsetzung)

Wir fassen die berechenbaren Funktionen und berechenbaren partiellen Funktionen in folgenden Klassen zusammen:

$$\mathrm{FREC} = \{f \mid f \text{ ist eine berechenbare (totale) Funktion}\}$$

$$\mathrm{FREC}_p = \{f \mid f \text{ ist eine berechenbare partielle Funktion}\}$$

Bemerkung

Offensichtlich gilt $\mathrm{FREC} \subsetneq \mathrm{FREC}_p$

Beispiel

- Bezeichne x^+ den lexikografischen Nachfolger von $x \in \Sigma^*$
- Für $\Sigma = \{0, 1\}$ ergeben sich beispielsweise folgende Werte:

x	ε	0	1	00	01	10	11	000	$\cdots$
x^+	0	1	00	01	10	11	000	001	$\cdots$

- Betrachte die auf Σ^* definierten partiellen Funktionen f_1, f_2, f_3, f_4 mit

$$f_1(x) = 0$$
$$f_2(x) = x$$
$$f_3(x) = x^+$$

und

$$f_4(x) = \begin{cases} \uparrow, & x = \varepsilon \\ y, & x = y^+ \end{cases}$$

- Da f_1, f_2, f_3, f_4 berechenbar sind, gehören die totalen Funktionen f_1, f_2, f_3 zu FREC und die partielle Funktion f_4 zu FREC_p
- Da f_4 keine totale Funktion ist, gehört f_4 nicht zu FREC ◁

Partielle charakteristische Funktionen

Für eine Sprache $A \subseteq \Sigma^*$ ist $\chi_A : \Sigma^* \to \{0,1\}$ mit

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

die charakteristische Funktion von A

Definition

- Die partielle charakteristische Funktion von A ist $\hat{\chi}_A : \Sigma^* \to \{1\} \cup \{\uparrow\}$ mit

$$\hat{\chi}_A(x) = \begin{cases} 1, & x \in A \\ \uparrow, & x \notin A \end{cases}$$

- A heißt rekursiv aufzählbar, falls $A = \varnothing$ oder das Bild $img(f)$ einer (totalen) berechenbaren Funktion $f : \Gamma^* \to \Sigma^*$ ist

Charakterisierung der rekursiv aufzählbaren Sprachen

Satz

Folgende Eigenschaften sind für eine Sprache $A \subseteq \Sigma^*$ äquivalent:

1. A ist semi-entscheidbar (d.h. A wird von einer DTM akzeptiert)
2. A wird von einer 1-DTM akzeptiert
3. A ist vom Typ 0
4. A wird von einer NTM akzeptiert
5. A ist rek. aufzählbar (d.h. $A = \varnothing$ oder $A = img(f)$ für eine Fkt. $f \in \mathrm{FREC}$)
6. $\hat{\chi}_A$ ist berechenbar (d.h. $\hat{\chi}_A \in \mathrm{FREC}_p$)
7. es gibt eine DTM M mit $A = dom(M)$

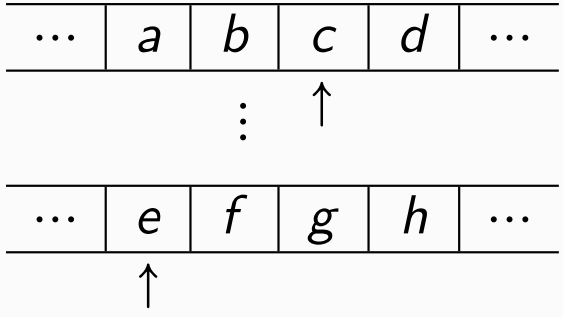
Beweis

Die Implikationen 2 $\Rightarrow$ 3 $\Rightarrow$ 4 werden in den Übungen gezeigt.
Hier zeigen wir 1 $\Rightarrow$ 2 und 4 $\Rightarrow$ 5 $\Rightarrow$ 6 $\Rightarrow$ 7 $\Rightarrow$ 1

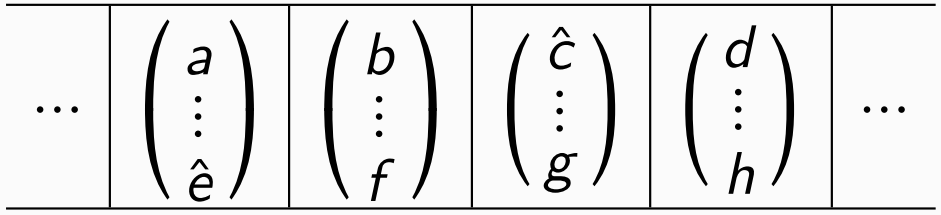
Simulation einer k-DTM durch eine 1-DTM

Beweis von ❶ $\Rightarrow$ ❷: $\{L(M) \mid M \text{ ist eine DTM}\} \subseteq \{L(M) \mid M \text{ ist eine 1-DTM}\}$

- Sei $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ eine k-DTM mit $L(M) = A$
- Wir konstruieren eine 1-DTM $M' = (Z', \Sigma, \Gamma', \delta', z_0, E)$ für A
- M' simuliert M, indem sie jede Konfiguration K von M der Form



durch eine Konfiguration K' folgender Form nachbildet:



Simulation einer k-DTM durch eine 1-DTM

Beweis von ❶ $\Rightarrow$ ❷: $\{L(M) \mid M \text{ ist eine DTM}\} \subseteq \{L(M) \mid M \text{ ist eine 1-DTM}\}$

- Hierzu arbeitet M' mit dem Alphabet

  $$\Gamma' = \Gamma \cup (\Gamma \cup \hat{\Gamma})^k, \text{ wobei } \hat{\Gamma} = \{\hat{a} \mid a \in \Gamma\} \text{ ist}$$

- Bei Eingabe $x = x_1 \dots x_n$ erzeugt M' zuerst die der Startkonfiguration

  $$K_x = (q_0, \varepsilon, x_1, x_2 \dots x_n, \varepsilon, \sqcup, \varepsilon, \dots, \varepsilon, \sqcup, \varepsilon)$$

  von M bei Eingabe x entsprechende Konfiguration

$$K'_x = q'_0 \begin{pmatrix} \hat{x}_1 \\ \hat{\sqcup} \\ \vdots \\ \hat{\sqcup} \end{pmatrix} \begin{pmatrix} x_2 \\ \sqcup \\ \vdots \\ \sqcup \end{pmatrix} \cdots \begin{pmatrix} x_n \\ \sqcup \\ \vdots \\ \sqcup \end{pmatrix}$$

Simulation einer k-DTM durch eine 1-DTM

Beweis von ❶ $\Rightarrow$ ❷: $\{L(M) \mid M \text{ ist eine DTM}\} \subseteq \{L(M) \mid M \text{ ist eine 1-DTM}\}$

- Dann simuliert M' jeweils einen Schritt von M durch folgende Sequenz von Rechenschritten:
  - Zuerst geht M' solange nach rechts, bis sie alle mit $\hat{}$ markierten Zeichen (z.B. $\hat{a}_1, \ldots, \hat{a}_k$) gefunden hat
  - Diese Zeichen speichert M' in ihrem Zustand
  - Anschließend geht M' wieder nach links und realisiert dabei die durch $\delta(q, a_1, \ldots, a_k)$ vorgegebene Anweisung von M
  - Dabei speichert M' den aktuellen Zustand q von M ebenfalls in ihrem Zustand
- Sobald M in einen Endzustand übergeht, wechselt M' ebenfalls in einen Endzustand und hält
- Somit gilt $L(M') = L(M)$ □

Charakterisierung der rekursiv aufzählbaren Sprachen

Beweis von ❹ ⇒ ❺: $\{L(M) \mid M \text{ ist eine NTM}\} \subseteq \{A \mid A \text{ ist rek. aufzählbar}\}$

- Sei $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ eine k-NTM und sei $A = L(M) \neq \varnothing$
- Sei $\tilde{\Gamma}$ das Alphabet $Z \cup \Gamma \cup \{\#\}$
- Wir kodieren eine Konfiguration $K = (q, u_1, a_1, v_1, \ldots, u_k, a_k, v_k)$ durch das Wort

  $$code(K) = \#q\#u_1\#a_1\#v_1\# \ldots \#u_k\#a_k\#v_k\#$$

  und eine Rechnung $K_0 \vdash \cdots \vdash K_t$ durch $code(K_0) \ldots code(K_t)$
- Dann lassen sich die Wörter von A durch folgende Funktion $f : \tilde{\Gamma}^* \to \Sigma^*$ aufzählen (dabei ist x_0 ein beliebiges Wort in A):

  $$f(w) = \begin{cases} x, & w \text{ kodiert eine akz. Rechnung } K_0 \vdash \cdots \vdash K_t \text{ von} \\ & M(x), \text{ d.h. } K_0 = K_x \text{ und } K_t \in E \times (\Gamma^* \times \Gamma \times \Gamma^*)^k \\ x_0, & \text{sonst} \end{cases}$$

- Da f total und berechenbar ist, ist $A = img(f)$ rekursiv aufzählbar □

Charakterisierung der rekursiv aufzählbaren Sprachen

Beweis von ❺ ⇒ ❻: $\{A \mid A \text{ ist rek. aufzählbar}\} \subseteq \{A \mid \hat{\chi}_A \in \mathrm{FREC}_p\}$

- Sei M eine DTM, die eine Fkt. $f : \Gamma^* \to \Sigma^*$ mit $A = img(f)$ berechnet
- Dann wird $\hat{\chi}_A$ von der DTM M' berechnet, die bei Eingabe x
  - der Reihe nach für alle $w \in \Gamma^*$ das Wort $f(w)$ berechnet und
  - den Wert 1 ausgibt, sobald $f(w) = x$ ist □

Beweis von ❻ ⇒ ❼: $\{A \mid \hat{\chi}_A \in \mathrm{FREC}_p\} \subseteq \{dom(M) \mid M \text{ ist eine DTM}\}$

- Sei M eine DTM, die $\hat{\chi}_A$ berechnet
- Da $dom(\hat{\chi}_A) = A$ ist, folgt $A = dom(M)$ □

Beweis von ❼ ⇒ ❶: $\{dom(M) \mid M \text{ ist eine DTM}\} \subseteq \{L(M) \mid M \text{ ist eine DTM}\}$

- Sei $A = dom(M)$ für eine DTM M
- Dann gilt $A = L(M')$ für die DTM M', die M simuliert und genau dann in einen Endzustand übergeht, wenn M hält □

Charakterisierung der entscheidbaren Sprachen

Satz

Folgende Eigenschaften sind äquivalent:

1. A ist entscheidbar (d.h. A wird von einer DTM akzeptiert, die alle Eingaben entscheidet)
2. die charakteristische Funktion χ_A von A ist berechenbar
3. A wird von einer 1-DTM akzeptiert, die bei allen Eingaben hält
4. A wird von einer NTM akzeptiert, die bei allen Eingaben hält
5. A und $\bar{A}$ sind semi-entscheidbar

Beweis

Die Äquivalenz der Bedingungen 1 bis 4 wird in den Übungen gezeigt. Hier zeigen wir nur die Äquivalenz dieser vier Bedingungen zu 5

Charakterisierung der entscheidbaren Sprachen

Beweis von ❶ ⇒ ❺: REC ⊆ RE ∩ co-RE

- Falls A entscheidbar ist, ist χ_A wegen ❶ ⇒ ❷ berechenbar
- Mit χ_A ist auch $\chi_{\bar{A}}$ berechenbar, d.h. A und $\bar{A}$ sind wegen ❷ ⇒ ❶ entscheidbar und damit auch semi-entscheidbar

Beweis von ❺ ⇒ ❶: RE ∩ co-RE ⊆ REC

- Sei $A \in \text{RE} \cap \text{co-RE}$ und seien M_A und $M_{\bar{A}}$ DTMs, die $\hat{\chi}_A$ und $\hat{\chi}_{\bar{A}}$ berechnen
- Betrachte die DTM M, die abwechselnd M_A und $M_{\bar{A}}$ für jeweils einen weiteren Rechenschritt simuliert und
  - in einem Endzustand hält, sobald $M_A(x)$ hält, sowie
  - in einem Nichtendzustand hält, sobald $M_{\bar{A}}(x)$ hält
- Da jede Eingabe x entweder in $dom(\hat{\chi}_A) = A$ oder in $dom(\hat{\chi}_{\bar{A}}) = \bar{A}$ enthalten ist, hält M bei allen Eingaben
- Da zudem $L(M) = A$ ist, folgt $A \in \text{REC}$ □

Kodierung (Gödelisierung) von Turingmaschinen

- Um Eigenschaften von TMs algorithmisch untersuchen zu können, müssen wir TMs als Teil der Eingabe kodieren
- Sei $M = (Z, \Sigma, \Gamma, \delta, q_0, E)$ eine 1-DTM mit
  - Zustandsmenge $Z = \{q_0, \ldots, q_m\}$ (o.B.d.A. sei $E = \{q_m\}$),
  - Eingabealphabet $\Sigma = \{0, 1\}$ und
  - Arbeitsalphabet $\Gamma = \{a_0, \ldots, a_l\}$,
    wobei wir o.B.d.A. $a_0 = 0$, $a_1 = 1$ und $a_2 = \sqcup$ annehmen
- Dann kodieren wir eine Anweisung $q_i a_j \to q_{i'} a_{j'} D$ durch das Wort

$$\#bin(i)\#bin(j)\#bin(i')\#bin(j')\#b_D\#$$

- Dabei ist $bin(n)$ die Binärdarstellung von n und

$$b_D = \begin{cases} 0, & D = N \\ 1 & D = L \\ 10, & D = R \end{cases}$$

Kodierung von Turingmaschinen

- M lässt sich nun als ein Wort über dem Alphabet $\{0, 1, \#\}$ kodieren, indem wir die Anweisungen von M in kodierter Form auflisten
- Kodieren wir die Zeichen $0, 1, \#$ binär (z.B. $0 \mapsto 00$, $1 \mapsto 01$, $\# \mapsto 10$), so gelangen wir zu einer Binärkodierung w_M von M
- Die durch die Binärzahl $w_M = b_n \dots b_0$ repräsentierte natürliche Zahl $(w_M)_2 = \sum_{i=0}^{n} b_i 2^i$ wird auch die Gödel-Nummer von M genannt
- M_w ist durch Angabe von w_M bzw. $(w_M)_2$ bis auf die Benennung ihrer Zustände und der Arbeitszeichen in $\Gamma \setminus \{\sqcup, 0, 1\}$ eindeutig bestimmt
- Ganz analog lassen sich auch k-DTMs mit $k > 1$ sowie NTMs binär kodieren
- Umgekehrt können wir jedem Binärstring $w \in \{0, 1\}^*$ eine DTM M_w wie folgt zuordnen (dabei ist M_0 eine beliebige, aber fest gewählte DTM):

$$M_w = \begin{cases} M, & \text{falls eine DTM } M \text{ mit } w_M = w \text{ existiert} \\ M_0, & \text{sonst} \end{cases}$$

Unentscheidbarkeit des Halteproblems

Definition

Das Halteproblem ist die Sprache

$$H = \left\{ w\#w' \;\middle|\; \begin{array}{l} w, w' \in \{0,1\}^* \text{ und} \\ \text{die DTM } M_w \text{ hält} \\ \text{bei Eingabe } w' \end{array} \right\}$$

und das spezielle Halteproblem ist

$$K = \left\{ w \in \{0,1\}^* \;\middle|\; \begin{array}{l} \text{die DTM } M_w \\ \text{hält bei Eingabe } w \end{array} \right\}$$

χ_H	w_1	w_2	w_3	$\cdots$
w_1	0	1	0	$\cdots$
w_2	0	1	1	$\cdots$
w_3	1	1	0	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

χ_K				
w_1	**0**			
w_2		**1**		
w_3			**0**	
$\vdots$				$\ddots$

Satz

$K, H \in \mathrm{RE}$

Semi-Entscheidbarkeit des (speziellen) Halteproblems

Beweis von $K, H \in \mathrm{RE}$

- Sei w_h die Kodierung einer DTM, die sofort hält, und betrachte die Funktionen $f_K : \{0,1\}^* \to \{0,1\}^*$ und $g_H : \{0,1,\#\}^* \to \{0,1,\#\}^*$ mit

$$f_K(x) = \begin{cases} w, & x \text{ ist die Binärkodierung einer haltenden Rechnung} \\ & \text{einer DTM } M_w \text{ bei Eingabe } w, \\ w_h, & \text{sonst} \end{cases}$$

und

$$g_H(x) = \begin{cases} w\#w', & x = w\#x' \text{ und } x' \text{ ist die Binärkodierung einer hal-} \\ & \text{tenden Rechnung der DTM } M_w \text{ bei Eingabe } w', \\ w_h\#\varepsilon, & \text{sonst} \end{cases}$$

- Da f_K und g_H in FREC sind und $img(f_K) = K$ sowie $img(g_H) = H$ ist, folgt $K, H \in \mathrm{RE}$ □

Unentscheidbarkeit des speziellen Halteproblems

Satz

$\bar{K} \notin \text{RE}$ und somit $\text{REC} \subsetneq \text{RE} \neq \text{co-RE}$

Beweisidee

- Sei $B = (b_{ij})$ die durch $b_{ij} = \chi_H(w_i \# w_j) \in \{0,1\}$ definierte Binärmatrix
- Dann kann keine Zeile $b_{i1} b_{i2} \ldots$ von B mit der invertierten Diagonalen $\bar{b}_{11} \bar{b}_{22} \ldots$ von B übereinstimmen, da sonst $b_{ii} = \bar{b}_{ii}$ sein müsste
- Da die i-te Zeile von B wegen

  $$b_{ij} = \chi_H(w_i \# w_j) = \chi_{dom(M_{w_i})}(w_j)$$

  die Binärsprache $dom(M_{w_i}) \in \text{RE}$ und die invertierte Diagonale wegen

  $$\bar{b}_{ii} = \chi_{\bar{H}(w_i \# w_i)} = \chi_{\bar{K}}(w_i)$$

  die Sprache $\bar{K}$ repräsentiert, folgt $\bar{K} \neq dom(M_{w_i})$ für alle $i \geq 1$
- Dies impliziert $\bar{K} \notin \text{RE}$, da die Gesamtheit der Zeilen von B wegen

  $$\{dom(M_{w_i}) \mid i \geq 1\} = \{A \subseteq \{0,1\}^* \mid A \in \text{RE}\}$$

  die Klasse aller Binärsprachen in RE repräsentiert

Unentscheidbarkeit des speziellen Halteproblems

Beweis von $\bar{K} \notin \mathrm{RE}$

- Angenommen, die Sprache

$$\bar{K} = \{w \in \{0,1\}^* \mid M_w(w)\uparrow\} \qquad (*)$$

wäre semi-entscheidbar

- Dann existiert eine DTM M_{w_i} mit

$$dom(M_{w_i}) = \bar{K} \qquad (**)$$

- Dies führt jedoch auf einen Widerspruch:

$$w_i \in \bar{K} \underset{(*)}{\Leftrightarrow} M_{w_i}(w_i)\uparrow \Leftrightarrow w_i \notin dom(M_{w_i}) \underset{(**)}{\Leftrightarrow} w_i \notin \bar{K} \quad \lightning$$

□

χ_H	w_1	w_2	w_3	$\cdots$
w_1	**0**	1	0	$\ldots$
w_2	0	**1**	1	$\ldots$
w_3	1	1	**0**	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	
w_i	**1**	**0**	**1**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Bemerkung

- Die Methode in obigem Beweis wird als Diagonalisierung bezeichnet
- Mit dieser Beweistechnik lässt sich auch eine Sprache in $\mathrm{REC} \setminus \mathrm{CSL}$ definieren (siehe Übungen)